Department of the Army Pamphlet 25–1–2

Information Management

Information Technology Contingency Planning

Headquarters
Department of the Army
Washington, DC
16 November 2006

UNCLASSIFIED

SUMMARY of CHANGE

DA PAM 25-1-2
Information Technology Contingency Planning

This new Department of the Army Pamphlet, dated 16 November 2006--

- Discusses the principles of information technology contingency planning, types of plans that comprise an overall continuity of operations plan, of information technology contingency planning in regards to the system development life cycle, and information technology contingency planning at the installation level as a foundation for the rest of the publication (chap 2).

- Covers information technology contingency plan elements, including the information technology contingency statement; business impact analysis; emergency policies and procedures; recovery strategies; plan testing, training, and exercises; and plan maintenance (chap 3).

- Discusses emergency procedures and the phases of contingency operations including the development of information technology contingency plan supporting information, emergency actions, the notification/activation phase, the recovery phase, the reconstitution phase, and the development of plan appendixes (chap 4).

- Provides guidance regarding information technology contingency planning for specific systems such as desktop computers and portable systems, servers, Web sites, using Army Knowledge Online, local area networks, wide area networks, distributed systems, and mainframe systems (chap 5).

- Documents guidance regarding information technology contingency plan services including contingency support for information services, emergency information technology services, mobilization information support services, alternate sites service support, and teleworking (chap 6).

- Provides guidance on information technology system priority including a prioritization of services and a prioritization scheme (chap 7).

- Provides an information technology contingency plan template for use as a general guide to developing an information technology contingency plan (app B).

Headquarters
Department of the Army
Washington, DC
16 November 2006

***Department of the Army Pamphlet 25–1–2**

Information Management

Information Technology Contingency Planning

By Order of the Secretary of the Army:

PETER J. SCHOOMAKER
General, United States Army
Chief of Staff

Official:

JOYCE E. MORROW
Administrative Assistant to the Secretary of the Army

History. This publication is a new Department of the Army pamphlet.

Summary. This pamphlet provides procedures for developing and exercising IT contingency plans. This pamphlet supports AR 25–1 in implementing Title 10, United States Code, and Section 1401, Title 40, United States Code (Public Law 104–106, the Clinger-Cohen Act, formerly Division E, Technology Management Reform Act). Procedures for operational security and the development of emergency relocation groups are covered in other publications and are not included in this publication.

Applicability. This pamphlet applies to the Active Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve, unless otherwise stated. This pamphlet applies to nontactical command, control, communications, and computers/information technology at all Army installations, activities, and communities.

Proponent and exception authority. The proponent of this pamphlet is the Chief Information Officer/G–6. The Chief Information Officer/G–6 has the authority to approve exceptions or waivers to this pamphlet that are consistent with controlling law and regulations. The Chief Information Officer/G–6 may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this pamphlet by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through higher headquarters to the policy proponent. Refer to AR 25–30 for specific guidance.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to the Chief Information Officer/G–6, CIO Policy Division (SAIS–GKP), 107 Army Pentagon, Washington, DC 20310–0107.

Distribution. This publication is available in electronic media only and is intended for command levels C, D, and E for the Active Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve.

Contents (Listed by paragraph and page number)

*This publication is a new Department of the Army pamphlet.

UNCLASSIFIED

Contents—Continued

Contents—Continued

Figure List

Glossary

Chapter 1
IT Contingency Planning

1–1. Purpose
This pamphlet provides operational procedures and practical guidance to information technology (IT) contingency planning for Army organizations developing, using, or maintaining nontactical IT services, products, and support. IT contingency planning is general support systems and contingency plans for major applications and support systems. The primary focus of this document is the implementation of policies mandated by Army Regulation (AR) 25–1, AR 25–2, AR 70–1, and AR 500–3 and Department of Defense Directive (DODD) 8500.1 and Department of Defense Instruction (DODI) 8500.2. Its emphasis is on identifying and describing implementing procedures, explicit and implied, stemming from Defense policies and Federal authorities, to include Title 40, United States Code, Chapter 25, Subchapter III) (40 USC 1401) (the Clinger-Cohen Act); 44 USC 3601 (the Federal Information Security Management Act of 2002); Federal Preparedness Circular (FPC) 65; 10 USC 2224 (the National Defense Authorization Act for FY 2000); and Office of Management and Budget (OMB) Circular A–130.

1–2. References
Required and related publications and prescribed and referenced forms are listed in appendix A.

1–3. Explanation of abbreviations and terms
Abbreviations and special terms used in this publication are explained in the glossary.

1–4. Exceptions
This pamphlet does not address operations security or the development of emergency relocation groups, both of which are covered by AR 500–3.

1–5. General
The scope of this pamphlet includes all organizational levels. The importance of regularly exercising the plans generated using this pamphlet cannot be overstated. An essential principle is having a single organization at the installation, community, or corresponding entity charged with overseeing IT contingency planning.

Chapter 2
Principles of IT Contingency Planning

2–1. Risk management
a. Risk management is not an event but a process. An ongoing commitment is essential to effective risk management as a building block of IT contingency planning.

b. Risk management includes an array of activities used to identify, control, and mitigate risks to IT systems and the ability to provide IT services. A thorough risk assessment identifies system vulnerabilities, threats, and current controls with an attempt to determine the risk based on the likelihood and threat impact.

c. All too often, risk management falls on information management offices to implement. Risk management is a team activity and should begin by forming a risk management team (RMT). The RMT includes representatives of management, user departments, and the information management officer, to include those responsible for information assurance (IA) issues. The RMT divides the information activities among the functional areas of the organization and involves representatives from the respective departments in the asset identification process.

d. The three major components of a risk management program are—

(1) Performing a risk assessment to identify the organization's information assets and the threats to each asset.

(a) The RMT begins by identifying the organization's information assets. Information assets include information systems and the data they contain, records and documentation, and people. The criticality of each asset is determined by the team based on a predefined scale (such a critical, high, medium, or low). The RMT considers the organization's legal requirements when quantifying criticality. The criticality of each asset determines the level of controls that are required.

(b) For each information asset, the RMT considers any methods used to access, collect, store, use, transmit, protect, and dispose of the information. The RMT completes a risk assessment exercise for each information asset to identify and enumerate the foreseeable threats for each method. For each applicable method, the RMT further considers any threats that impact the asset's confidentiality, integrity, and availability. Each threat then undergoes an evaluation by the RMT based on the probability of occurrence (high, moderate, or low). Within each asset, the threats with the highest probability of occurrence require the strongest controls**.**

(c) In order to maintain the integrity of the assessment process, the RMT organizes the risk assessment records

according to the respective information assets. The documentation cross-references to the respective systems that could impact the asset.

(d) The RMT prioritizes their activities for identifying and implementing controls and evaluating control effectiveness based on the criticality of the assets and the probability of the threats. The most critical assets and the highest probable threats receive the most attention.

(2) Identifying and implementing controls to mitigate the threats.

(a) Once the risk assessment has been completed, the RMT identifies the existing controls for each identified threat.

(b) The team identifies and documents any existing (or newly implemented) controls that mitigate or eliminate the corresponding risk.

(c) In places where the organization does not have controls, the committee develops and implement new controls.

(3) Evaluating the controls to assess their effectiveness.

(a) On the basis of the controls identified for each threat, the RMT assesses whether the controls sufficiently reduce or eliminate the risks associated with the threat. The organization develops a control testing and monitoring plan to test each control identified.

(b) The RMT may determine that additional controls are required. When weak or missing controls have been identified for specific threats, the team plans and implements procedures to expand or develop missing controls. Once these controls are implemented, they are evaluated following the same control evaluation process used on the existing controls.

e. Risk management is a continual process that must receive ongoing attention.

(1) Once the initial risk assessment has been completed, the RMT develops a schedule for reassessing risk. The schedule is based on the criticality of each information asset and includes opportunities for expanding the list of information assets.

(2) At a minimum, controls are retested annually. Complex controls are tested more often. Each critical information asset is re-evaluated semiannually. All information assets are re-evaluated whenever there has been a significant change to the systems, records, or people that comprise that asset. Software tools can assist business leaders in performing a risk assessment but cannot replace sound risk management processes.

(3) The RMT maintains a centralized record of risk-management activities. The risk-management process is typically evaluated with equal importance to the risk management results when critiqued by internal and external auditors, regulators, and other evaluation groups. The risk-management record can also be used to quantify risk management results.

2–2. Types of plans

The scope of what is included as part of IT contingency planning has been confusing at times because a definition of it has often been unavailable. This section identifies types of plans and describes their purpose and scope relative to IT contingency planning. Table 2–1 summarizes the types of plans, as well as their purpose and scope.

a. IT contingency planning. This represents an array of activities that sustain and recover IT systems and services following an emergency.

(1) An organization would ultimately use an entire suite of plans in order to properly prepare response, recovery, and continuity activities for disruptions affecting the organization's IT systems, business processes, and facilities.

(2) Because there is a definite relationship between an IT system and the business process it supports, care must be taken to ensure that recovery strategies and supporting resources neither negate nor duplicate efforts.

b. Business continuity plan (BCP). The BCP focuses on sustaining an organization's business functions (continuity of business) during and after a disruption. IT systems are considered in the BCP in terms of their support to the business processes.

c. Business recovery plan (BRP). The BRP, also known as a business resumption plan, addresses the restoration of business processes after an emergency but, unlike the BCP, does not include procedures to ensure the continuity of mission essential functions (MEFs) throughout the emergency or disruption.

d. Continuity of operations plan (COOP). The COOP focuses on restoring an organization's (usually a headquarters element's) MEFs using alternate procedures and performing those functions for up to 30 days before returning to precontingency-level operations. Alternate procedures may be executed at an alternate site or at the normal operational site. Because the COOP emphasizes the recovery of an organization's operational capability, the plan does not necessarily include IT operations.

e. Continuity of support plan/IT contingency plan. Continuity of support plan/IT contingency plan. OMB Circular A–130, Appendix III, requires the development and maintenance of continuity support plans for general support systems and contingency plans for major applications. This planning guide considers continuity of support planning to be synonymous with IT contingency planning. Because an IT contingency plan must be developed for each major application and general support system, multiple contingency plans may be maintained within the organization's BCP.

f. Crisis communications plan. The crisis communications plan typically designates specific individuals as the only

authority for answering questions from the public regarding contingency response and may include procedures for disseminating status reports to personnel and the public.

g. Cyber incident response plan. The cyber incident response plan establishes procedures to address cyber attacks against an organization's IT systems.

h. Disaster recovery plan (DRP). As suggested by its name, the DRP applies to major, usually catastrophic, events that deny access to the usual facility for an extended period. Frequently, DRP refers to an IT-focused plan designed to restore operability of systems, applications, and an IT contingency plan; however, the DRP is narrower in scope and does not address minor disruptions that do not require relocation.

i. Occupant emergency plan (OEP). The OEP provides the response procedures for occupants of a facility in the event of a situation posing a potential threat to the health and safety of personnel, the environment, or property.

Table 2–1
Types of contingency-related plans

Plan	Purpose	Scope
BCP	Provide procedures for sustaining essential business operations while recovering from a significant disruption	Addresses business processes; IT addressed based only on its support for business process
BRP (or business resumption plan)	Provide procedures for recovering business operations immediately following a disaster	Addresses business processes; not IT focused; IT addressed based only on its support for business process
COOP	Provide procedures and capabilities to sustain an organization's essential, strategic functions using alternate procedures for up to 30 days	Addresses the subset of an organization's missions that are deemed most critical; usually written at headquarters level; not IT focused
IT contingency plan continuity of support plan/IT contingency plan	Provide procedures and capabilities for recovering a major application or general support system	Addresses IT system disruptions; not business process focused
Crisis communications plan	Provides procedures for disseminating status reports to personnel and the public	Addresses communications with personnel and the public; not IT focused
Cyber incident response plan	Provide strategies to detect, respond to, and limit consequences of malicious cyber incident	Focuses on information security responses to incidents affecting systems and/or networks
DRP	Provide detailed procedures to facilitate recovery of capabilities at an alternate site	Often IT focused; limited to major disruptions with long-term effects
OEP	Provide coordinated procedures for minimizing loss of life or injury and protecting property damage in response to a physical threat	Focuses on personnel and property particular to the specific facility; not business process or IT system functionality based. Usually includes emergency evacuation and shelter-in-place planning

2–3. Information technology contingency planning and system development life cycle

The system development life cycle refers to the full scope of activities conducted by system owners that are associated with a system during its life span. Although contingency planning is associated with activities occurring in the operation/maintenance phase, contingency measures is identified and integrated at all phases of the computer system life cycle.

a. Initiation phase. IT contingency planning requirements are considered when a new IT system is being conceived.

(1) In the initiation phase, systems requirements are identified and matched to their related operational processes, and initial contingency requirements may become apparent.

(2) During this phase, the new IT systems also is evaluated against all other existing and planned IT systems to determine its appropriate recovery priority.

b. Development/acquisition phase. As initial concepts develop into system designs, specific contingency solutions may be incorporated. As in the initiation phase, contingency measures included in this phase reflect system and operational requirements. In cases where applications and systems are developed by a program manager, a standard method for contingency planning is provided to customers. See AR 70–1 for requirements that mission critical/mission essential (MC/ME) IT systems be registered with the Army Chief Information Officer (CIO)/G–6 and Department of Defense CIO. See AR 70–75 for information on the requirements for survivability of MC/ME systems.

(1) The design incorporates redundancy and robustness directly into the system architecture to optimize reliability, maintainability, and availability during the operation/maintenance phase.

(2) If multiple applications are hosted within the new general support system, individual priorities for those

applications are set to assist with selecting the appropriate contingency measures and sequencing for the recovery execution.

(3) Redundant communications paths, lack of single points of failure, enhanced fault tolerance of network components and interfaces, power management systems with appropriately sized backup power sources, load balancing, and data mirroring and replications to ensure a uniformly robust system are examples of contingency measures that need to be considered in this phase.

(4) If an alternate site is chosen as a contingency measure, requirements for the alternate site are addressed in this phase.

c. Implementation phase. Although the system is undergoing initial testing, contingency strategies also need to be tested to ensure that technical features and recovery procedures are accurate and effective.

(1) Testing contingency strategies requires that a test plan be formed.

(2) When these contingency measures have been verified, they must be clearly documented in the contingency plan.

d. Operations/maintenance phase. When the system is operational, users, administrators, and managers maintain a training and awareness program that covers the contingency plan procedures.

(1) Exercises and tests are conducted to ensure that the procedures continue to be effective.

(2) Regular backups should be conducted and stored offsite in accordance with procedures based on classification requirements.

(3) The plan is updated to reflect changes to procedures based on lessons learned.

(4) When IT systems are upgraded or modified, such as changes to external interfaces, these modifications are reflected in the contingency plan.

(5) Coordinating and documenting changes in the plan are made in a timely manner to maintain an effective plan.

e. Disposal phase. Contingency considerations must not be neglected because a computer system is retired and another system replaces it.

(1) Until the new system is fully tested, accredited, and operational (including its contingency capabilities), the original system's contingency plan remains ready for implementation.

(2) As legacy systems are replaced, they may provide a valuable backup capability if a loss or failure of the new system occurs.

(3) Legacy systems can be used as test systems for new applications, allowing potentially disruptive system flaws to be identified and corrected on nonoperational systems.

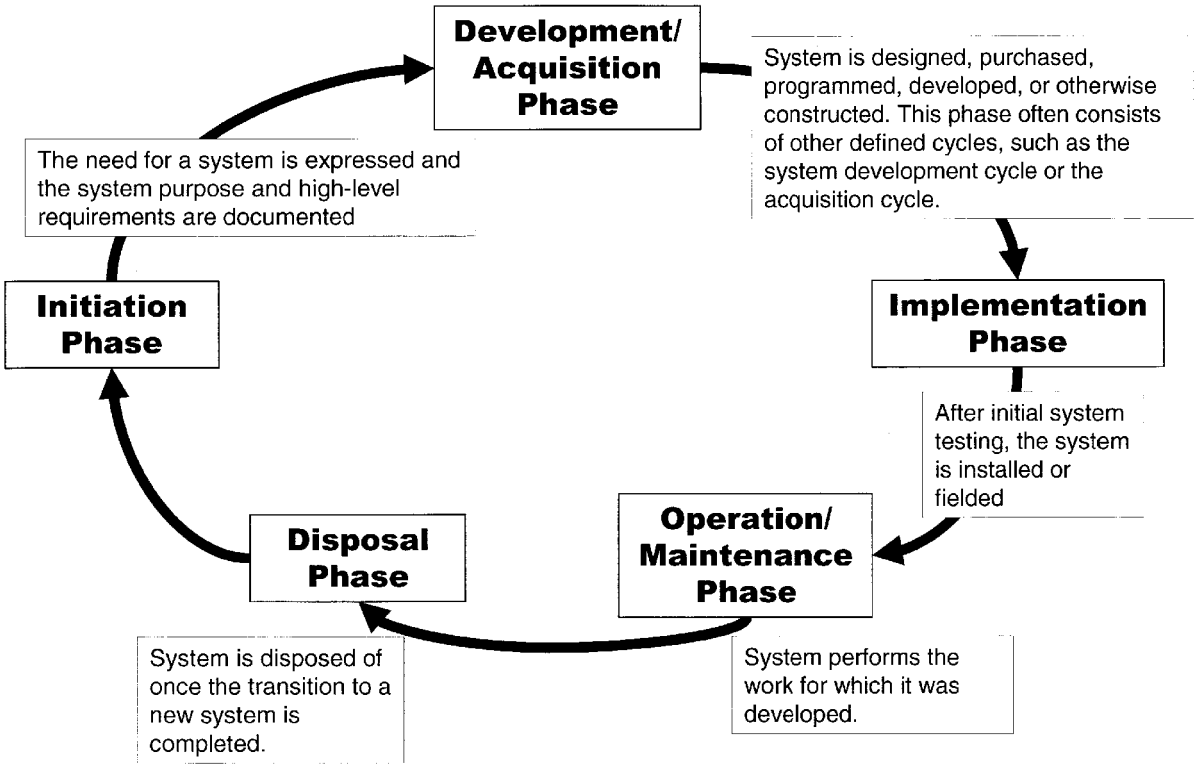


Figure 2–1. System development life cycle

2–4. Emergency and information technology contingency requirements.

a. IT contingency planning is a good business practice and one part of the fundamental mission of agencies as responsible and reliable public institutions.

b. The objectives of an IT contingency plan include—

(1) Preparation for meeting the challenges of threats identified during the risk assessment.

(2) Ensuring the continuous performance of an organization's MEFs/operations during an emergency.

(3) Protecting ME equipment, records, and other assets.

(4) Reducing or mitigating disruptions to operations.

(5) Reducing damage and losses.

(6) Achieving a timely and orderly recovery from an emergency and resumption of full service to customers.

c. A viable IT contingency capability is—

(1) Maintained at a high level of readiness.

(2) Capable of implementation both with and without warning.

(3) Operational no later than 12 hours after activation.

(4) Able to maintain sustained operations for up to 30 days.

(5) Ready to take maximum advantage of existing organization field infrastructures.

d. Agencies develop their IT contingency capabilities using a multiyear strategy and program management plan. This plan outlines the process the organization should follow to designate MEFs and resources, define short- and long-term IT contingency goals and objectives, forecast budgetary requirements, anticipate and address issues and potential obstacles, and establish planning milestones. A well-defined IT portfolio management and evaluation methodology for assessing continuity of operations and contingency planning as related to the existing baseline enterprise architecture should be well defined and understood. A lack of this understanding could result in a lack of funding and effort needed to implement effective and efficient approaches of crisis restoration across the IT enterprise and the inability of the

Army to provide and plan for contingency plan funding, IA, hardware and software applications for staff during crisis management scenario operations.

e. At a minimum, all organizational contingency capabilities encompass the following elements:

(1) *Plans and procedures.* An IT contingency plan is developed and documented and, when implemented, provides for continued performance of essential federal functions under all circumstances. At a minimum, the plan—

(a) Delineates MEFs and activities.

(b) Outlines a decision process for determining appropriate actions in implementing IT contingency plans and procedures.

(c) Establishes a roster of fully equipped and trained personnel with the authority to perform MEFs and activities.

(d) Includes procedures for employee advisories, alerts, and IT contingency plan activation, with instructions for relocation to predesignated facilities, with and without warning, during duty and nonduty hours.

(e) Provides for personnel accountability throughout the duration of the emergency.

(f) Provides for attaining operational capability within 12 hours.

(g) Establishes reliable processes and procedures to acquire resources necessary to continue MEFs and sustain operations for up to 30 days.

(2) *Identification of MEFs.* All agencies should identify their MEFs as the basis for IT contingency planning. MEFs are those functions that enable organizations to provide vital services. In identifying MEFs, agencies—

(a) Identify all functions performed by the organization and then determine which should be continued under all circumstances.

(b) Prioritize these MEFs.

(c) Establish staffing and resources requirements needed to perform MEFs.

(d) Identify MC data and systems necessary to conduct MEFs.

(e) Defer functions not deemed essential to immediate organizational needs until additional personnel and resources become available.

(f) Integrate supporting activities to ensure that MEFs can be performed as efficiently as possible during emergency relocation.

(3) *Delegation of authority.* To ensure rapid response to any emergency situation requiring IT contingency plan implementation, agencies predelegate authorities for making policy determinations and decisions at headquarters, field levels, and other organizational locations, as appropriate. These delegations of authority—

(a) Identify the programs and administrative authorities needed for effective operations at all organizational levels having emergency responsibilities.

(b) Identify the circumstances under which the authorities would be exercised.

(c) Document the necessary authorities at all points where emergency actions may be required, delineating the limits of authority and accountability.

(d) Explicitly state the authority of designated successors to exercise organizational direction, including any exceptions, and the successor's authority to redelegate functions and activities as appropriate.

(e) Indicate the circumstances under which delegated authorities would become effective and when they would terminate and generally predetermined delegations of authority would take effect when the usual channels of direction are disrupted and would terminate when these channels have resumed.

(f) Ensure that officials who may be expected to assume authorities in an emergency are trained to carry out their emergency duties.

(g) Specify responsibilities and authorities of individual organization representatives, such as those responsible for IA matters, designated to participate as members of interorganization contingency response teams. Figure 2–2 provides a sample contingency response team duty appointment letter.

(Insert Office Symbol) 16 March 2006

MEMORANDUM FOR See Distribution

SUBJECT: Announcement of Duty Appointment

1. Effective 16 March 2006, the following individuals are appointed to the (INSERT NAME OF INSTALLATION) DOIM Contingency Response Team:

a. Ms. (INSERT NAME) IT Contingency Plan Site Manager

b. Mr. (INSERT NAME) Support Coordinator

c. Ms. (INSERT NAME) Network Site Coordinator

d. Mr. (INSERT NAME) Applications Site Coordinator

e. Ms. (INSERT NAME) SIPR Site Coordinator

f. Mr. (INSERT NAME) Communications Site Coordinator

g. Ms. (INSERT NAME) IA Site Coordinator

2. Authority:

a. AR 25-1, Army Knowledge Management and Information Technology, 15 July 2005.

b. AR 25-2, Information Assurance, 14 November 2003.

c. AR 380-5, Department of the Army Information Security Program, 29 September 2000.

d. AR 500-3, Army Continuity of Operations (COOP) Program Policy and Planning, 12 April 2006.

e. DODD 3020.26, Defense Continuity Program (DCP), September 8, 2004.

f. DOD Instruction 3020.42, Defense Continuity Plan Development, 17 February 06

3. Purpose: To carry out assigned duties as prescribed in AR 25-1, AR 25-2, AR 380-5, AR 500-3, DODD 3020.26 and (INSERT NAME OF INSTALLATION/ACTIVITY) and DOIM organizational COOP policies in order to assure continuous operations of our local network and information systems (IS). Assigned personnel will assist in creating and maintaining plans for emergency response, backup operations, and post-disaster recovery of all DOIM critical IS. Assigned personnel will be responsible for implementing and executing appropriate actions in order to conduct emergency response, alternate operations and post-disaster recovery of all DOIM critical IS.

4. Period: Until released or relieved from appointment.

5. POC is Mr. (INSERT NAME), (INSERT CONTACT INFORMATION).

(INSERT SIGNATURE)
Director of Information Management

DISTRIBUTION:
Individual Operations Chief
Automations Chief
Network Operations Chief
Network Applications Chief
Information Assurance Chief
Communications Chief
Post Information Assurance Officer
Network Operations Center

Figure 2–2. Sample IT contingency duty appointment letter

(4) *Orders of succession.* Agencies are responsible for establishing, promulgating, and maintaining orders of succession to key positions. Such orders of succession are an essential part of an organization's IT contingency plan. Orders must be of sufficient depth to ensure the organization's ability to perform MEFs while remaining a viable part of the Federal Government through any emergency. Geographical dispersion is encouraged, consistent with the principle of providing succession to office in emergencies of all types. For more information, reference AR 500–3, paragraph 1–7*k*. Each organization should—

(a) Establish an order of succession to the position of organization head. A designated official serves as acting head of the organization until appointed by the President or relieved. Where a suitable field structure exists, appropriate personnel located outside the Washington, DC, area should be considered in the order of succession.

(b) Establish orders of succession to other key headquarters leadership positions.

(c) Establish, for agencies organized according to the standard Federal regional structure, an order of succession to the position of regional director or equivalent.

(d) Identify any limitation of authority based on delegations of authority to others.

(e) Describe orders of succession by positions or titles, rather than names of individuals.

(f) Include the orders of succession in the vital records of the organization.

(g) Revise orders of succession as necessary, and distribute revised versions promptly as changes occur. h) Establish the rules and procedures designated officials are to follow when facing the issues of succession to office in emergency situations.

(h) Include in succession procedures the conditions under which succession would take place, method of notification, and any temporal, geographical, or organizational limitations of authorities.

(i) Assign successors, to the extent possible, among the teams established to perform MEFs, to ensure that each team has an equitable share of duly constituted leadership.

(j) Conduct orientation programs to prepare successors for their emergency duties.

(5) Tests, training, and exercises. Testing, training, and exercising of IT contingency capabilities are essential to demonstrating and improving the ability of agencies to execute their IT contingency plans. Training familiarizes contingency staff members with the MEFs they may have to perform in an emergency. Tests and exercises serve to validate, or identify for subsequent correction, specific aspects of IT contingency plans, policies, procedures, systems, and facilities used in response to an emergency situation. Periodic testing also ensures that equipment and procedures are maintained in a constant state of readiness. All agencies must plan and conduct tests and training to demonstrate viability and interoperability of IT contingency plans. IT contingency test, training, and exercise plans provide for—

(a) Individual and team training of organization IT contingency staffs and emergency personnel to ensure currency of knowledge and integration of skills necessary to implement IT contingency plans and carry out MEFs. Team training should be conducted at least annually for IT contingency staffs on their respective IT contingency responsibilities.

(b) Internal organization testing and exercising of IT contingency plans and procedures to ensure the ability to perform MEFs and operate from designated alternate facilities). This testing and exercising should occur at least annually.

(c) Testing of alert and notification procedures and systems for any type of emergency at least quarterly.

(d) Refresher orientation for IT contingency arriving at an alternate operating facility. The orientation covers the support and services available at the facility, including communications and information systems for exchanging information if the usual operating facility is still functioning and administrative matters, including supervision, security, and personnel policies.

(e) Joint organization exercising of IT contingency plans, where applicable and feasible.

f. There are several factors to consider when implementing the IT contingency plan. Relocation may be required to accommodate a variety of emergency scenarios. While any of these scenarios involves unavailability of a facility, the distinction should be made between a situation requiring evacuation only and one dictating the need to implement IT contingency plans. An IT contingency plan includes the deliberate and preplanned movement of selected key principals and supporting staff to a relocation facility. As an example, a sudden emergency, such as fire or hazardous materials incident, may require the evacuation of an organization building with little or no advanced notice, but for only a short duration. Alternatively, an emergency so severe that an organization facility is rendered unusable and likely to remain so for a period long enough to significantly impact operations may require IT contingency plan implementation. Agencies should develop an executive decision process that allow for a review of the emergency and determination of the best course of action for response and recovery. This precludes premature or inappropriate activation of an organization contingency plan. One approach to ensuring a logical sequence of events in implementing an IT contingency plan is time phasing. Examples include scenarios in which—

(1) An organization headquarters is unavailable and operations can shift to a regional or field location.

(2) A single organization facility is temporarily unavailable and the organization can share one of its own facilities or that of another organization.

(3) Many, if not all, organizations need to evacuate an immediate area.

g. The following responsibilities are held by the heads of organizations and must be clearly outlined in IT contingency planning guidance and internal documents:

(1) Appointing an organization IT contingency program point of contact (POC).

(2) Developing an IT contingency multiyear strategy and program management plan.

(3) Developing, approving, and maintaining organization IT contingency plans and procedures for headquarters and all subordinate elements that provide for—

(a) Identification of organization MEFs.

(b) Predetermined delegations of authority and orders of succession.

(c) Contingency staffing to perform MEFs.

(d) Alternate operating facilities.

(e) Interoperable communications, information processing systems, and equipment.

(f) Protection of vital records and systems by—

1. Conducting tests and training of organization IT contingency plans, to include IT contingency and ME systems and equipment, to ensure timely and reliable implementation of IT contingency plans and procedures.

2. Participating in periodic interorganization IT contingency exercises to ensure effective interorganization coordination and mutual support.

3. Notifying the IT contingency program POC and other appropriate agencies upon implementation of IT contingency plans.

4. Coordinating intraorganization IT contingency efforts and initiatives with policies plans and activities related to terrorism and critical infrastructure protection under presidential policy guidance.

h. Plans need to consider force protection levels and the capability of employees and contractors to transit to and from the installation. Thought should be given to identifying employees and contractors and having predetermined and updated rosters available to Military Police and law enforcement officials to facilitate the movement of necessary personnel to effect contingency operations.

2–5. IT contingency planning at the installation level

a. Contingency plan characteristics at the installation level. The Director of Information Management (DOIM) is the focal point for IT contingency planning on Army installations. The DOIM or another responsible official operates as the COOP POC as required by AR 500–3, paragraph 1–7. The IT contingency plan should be fully aligned with the contingency plans of agencies such as Defense Information Systems Agency and the Network Enterprise Technology Command/9th Signal Command (Army), as required in AR 500–3. The installation networks and mission are part of the overall infrastructure designed to provide IT support to the Army in both peacetime and war. Local installations should also be prepared to support other garrison and military units in time of crisis by utilizing their own emergency plans. Armywide and installation-level planning is different in two key factors. Armywide contingency plans and operations are usually funded and mandated by regulation. IT contingency operations at the installation level are often poorly funded and based on doctrine from a variety of nonregulated sources. Keeping this in mind, successful and effective IT contingency plans at the installation level are characterized by the following attributes:

(1) Multiyear long-term planning is focused on near term needs. Long-term planning is needed and warranted in the areas of backbone infrastructure and contingency site location. True multiyear long-term contingency plans at the installation level can be unrealistic and difficult to manage. Technology infrastructure business processes are often in flux and usually mandated from higher headquarters, as are funding and future technologies. Consequently, it is almost impossible to plan what type of technology will be available for use in the long term. These limitations mean that contingency plans are be applied when business practices and technology changes are being planned for and implemented at the installation level. Examples of this type of planning include—

(a) When purchasing servers for a new business software initiative plan on purchasing one additional server of the same type. The additional server can be used for contingency as well as testing purposes. The additional server could be loaded with appropriate software and placed in an alternate location such as a hot or cold contingency site.

(b) When implementing a new technology service, create as-built documentation. Add all vendor information as well as system documentation to contingency plan documentation, to ensure a ready reference is available for rebuilding the service in an emergency.

(2) Minimum acceptable services required to support the installation IT infrastructure are determined. The DOIM, with the involvement of functional users and tenets, identifies all functions performed by the organization. It is the responsibility of the commander(s) to determine which functions should be given priority for restoration when the contingency plan is implemented. Required functions vary depending on the installations IT infrastructure and mission. Any support agreements between a DOIM and tenant/user should clearly state the responsibilities of the DOIM and tenant/user during a contingency situation.

(3) The installation contingency plan is integrated into daily operations. Few if any installation level activities have

a dedicated IT contingency planning site manager. Therefore, the use of smart books, as-built documents, troubleshooting checklists, and lessons learned should be maximized. Examples of this type of planning include—

(a) When replacing an out-of-date router with a newer model, develop a plan to ensure connectivity remains during the hardware changeover. Configuration changes and actions taken to maintain connectivity are documented and placed in the Installation IT contingency plan. This type of operation simulates and verifies the actions that would be taken during a contingency operation.

(b) Instead of taking mail servers off-line for maintenance, a method is developed to transfer users to a different server during the maintenance time period. This type of operation would be useful in documenting a method to move users to an off-site mail server during or after an emergency.

(4) Contingency plans are focused on more than servers and routers. Plans take into consideration the safety of workers, communications capabilities, and responses to other types of emergencies, including fire, hazardous materials, threats, attacks, and natural disasters. Vital records to include those needed for contingency operations are be identified and protected. Examples of non-IT-related planning factors include—

(a) Administrative equipment and materials that are needed in order to continue operations at the alternate site must be identified.

(b) Volunteer firefighters or emergency medical technicians on the installation staff need to be identified. These individuals can assist in a crisis until emergency crews arrive.

(c) The DOIM must have a copy of all current service agreements and contract numbers with their vital records. The records should include vendor name, address, telephone number (day and night), contact name (day and night), serial numbers of equipment under contract, contract number and expiration date.

(5) Creativity and inventiveness is embraced in all aspects of contingency planning and training. Encourage contingency team members to meet contingency goals and needs by experimenting with new ideas and continual learning. Develop multiple methods for achieving an individual task. Create multiple courses of action for each business contingency. If resources permit, run contingency scenarios in a lab environment. During an actual emergency, the contingency team would rely on the creative skills they rehearsed and honed during their planning and training. Examples of innovation in planning and training include—

(a) Contingency plans that can be practiced in a computer laboratory. If monies are not available for a complete laboratory a server running virtual machines can be utilized. Use retired routers, switches, computer and servers to create a new Active Directory network. Even if specifics are not able to be worked out, the courses of action can be.

(b) Cross-training members of the contingency response team. The contingency response team should be comprised of the best people within the organization. This environment is perfect for cross training the team. Have network administrators build servers using the rebuild and recovery documents created by members of the server recovery team. This tests documentation and cross trains team members at the same time. Remember that all members of the team may not be available during the actual emergency so cross training and documentation is imperative.

(c) Use of available resources to plan and train for failover procedures.

b. Planning steps. Contingency capabilities require substantial effort; as a result, plans should be developed and maintained utilizing the subject matter experts available. Plans are not made or maintained by one person working alone. A contingency plan outlines the process the agency is to follow to designate MEFs and resources, defines short- and near-term contingency plan goals and objectives, forecasts near-term budgetary requirements, anticipates and addresses issues and potential obstacles, and establishes planning milestones. A plan can be created using the following steps:

(1) *Develop a contingency planning policy statement.* This provides installation contingency response team members with the authority and guidance necessary to develop an effective contingency plan.

(2) *Conduct the business impact analysis (BIA).* The BIA helps team members identify and prioritize critical IT systems and components. See paragraph 2–5*d* for more specific information on the BIA.

(3) *Identify preventive controls.* Identify steps that can be taken immediately to reduce the effects of system disruptions and increase system availability and reduce contingency life cycle costs. Develop failover procedures.

(4) *Develop recovery strategies.* Recovery strategies help ensure that each system or supported business process can be recovered quickly and effectively following a disruption.

(5) *Develop the IT contingency plan.* The contingency plan should contain detailed guidance and procedures for restoring a damaged system or systems. Identify how long personnel can operate from an alternate or relocation site and develop the steps necessary when this time period expires.

(6) *Conduct testing, training, and exercises.* Testing the plan identifies planning gaps. Training prepares contingency response team members for plan activation. Combined, both activities improve plan effectiveness and overall team preparedness. As part of this training, encourage users to become familiar with remote access solutions available to them, including the use of Army Knowledge Online (AKO).

(7) *Maintain the plan.* The contingency plan should be a living document that is updated regularly to remain current with system changes. The installation needs to integrate IT contingency plan architecture and BRP into all IT purchases, system planning, and procurement.

c. Creation of an IT contingency plan policy. Before planning and organizing the contingency response team, a

formal policy letter and authority statement is created and approved by the garrison commander. The policy defines overall contingency objectives and establishes the organizational framework and responsibilities for IT contingency planning. The policy letter also addresses roles and responsibilities. The policy is supported with procedures covering training requirements, frequency of backups, offsite storage requirements, testing, and maintenance. A sample policy letter is included at figure 2–3.

DEPARTMENT OF THE ARMY
HEADQUARTERS, UNITED STATES ARMY GARRISON
(INSERT NAME/LOCATION OF ORGANIZATION)

COMMAND POLICY

(INSERT POLICY NUMBER)

(INSERT DATE)

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Continuity of Operations

1. REFERENCE:

a. AR 25-1, Army Knowledge Management and Information Technology Management, 15 July 2005
b. Army Regulation (AR) 25-2, Information Assurance, 14 November 2003
c. AR 380-5, Department of the Army Information Security Program, 29 September 2000
d. AR 500-3, Army Continuity of Operations (COOP) Program Policy and Planning, 12 April 2006
e. DOD Directive 3020.26, Defense Continuity Program (DCP), September 8, 2004
f. DOD Instruction 3020.42, Defense Continuity Plan Development, 17 February 06

2. APPLICABILITY. This policy applies to (INSERT APPLICABLE SYSTEMS) and the (INSERT NAME OF INSTALLATION) Directorate of Information Management (DOIM).

3. POLICY. In order to assure continuous operations of our local network and information systems (IS), the (INSERT NAME OF INSTALLATION) DOIM will create and maintain a plan for emergency response, backup operations, and post-disaster recovery for all critical IS. The plan will be incorporated as part of the (INSERT APPLICABLE SYSTEMS) and (INSERT NAME OF INSTALLATION) security program and will ensure the availability of critical resources and facilitate the continuity of operations. As a minimum the IT contingency plan will:

a. Provide for leadership successors and alternates and emergency delegation of authority
b. Safeguard essential resources, facilities, files, and records
c. Establish alternative emergency operating capabilities and facilities
d. Anticipate any emergency or crisis
e. Provide flexibility and responsiveness
f. Be capable of execution with little or no warning
g. Prioritize mission essential functions (MEF) that cannot be deferred
h. Identify functions that can be deferred until the situation permits their execution
i. Provide for alert and notification of selected personnel
j. The Directorate of Information Management will:

(1) Develop, coordinate, and maintain continuity plans, and shall validate, update, and reissue plans every 2 years, or more frequently as changes warrant.

(2) Identify and prioritize organizational MEF.

(3) Define emergency delegations of authority and orders of succession for key positions; identify and provide for alert/notification, movement, and training of continuity staffs; and address information technology and communications support to continuity operations.

(4) Identify relocation sites or platforms for component use during continuity threats or events. Site selection should consider geographical dispersion, and maximize co-location and dual-use facilities.

(5) Provide for the identification, storage, protection, and availability for use at relocation sites, the vital records, materiel, and databases required to execute MEF.

(6) Outline a decision process for determining appropriate actions in implementing continuity plans and procedures with or without warning, during duty and non-duty hours, and address the stand-down of continuity operations and transition back to standard operations.

(7) Ensure that continuity programs are adequately planned, programmed, and budgeted, and that (INSERT NAME OF APPLICABLE SYSTEMS) and (INSERT NAME OF INSTALLATION) unique requirements are specifically identified in their budgets. This shall include all assets and resources and the development, maintenance, and operations of facilities, communications, and transportation capabilities.

(8) Integrate continuity-related functions and activities into operations and exercises to assure that MEF can be performed across the spectrum of continuity threats or events.

(9) Test and exercise continuity plans at least annually or as otherwise directed, to evaluate program readiness.

(10) Integrate OPSEC requirements into continuity planning, execution, and operations.

4. EXPIRATION. This (INSERT NAME OF INSTALLATION) Garrison Command Policy Memorandum will remain in effect until superseded or rescinded.

(INSERT SIGNATURE)

(INSERT NAME OF COMMANDER) Commanding

Figure 2–3. Sample IT contingency plan policy letter

d. BIA. The BIA is thoroughly covered in paragraph 3–2 of this pamphlet. The BIA is one of the more difficult and time intensive portions of the continuity process. Many at the installation level may be tempted to skip or shortcut this process. The manager and planner of the contingency plan needs to pursue all avenues necessary to properly complete the BIA. A properly conducted BIA should reveal critical aspects of the continuity plan and the organization in general.

e. Preventive controls. The contingency plan planning and implementation process usually identify multiple organizational vulnerabilities. These critical business components and processes identified in the BIA are examined to determine controls that can be put in place immediately to prevent the system or process from being unavailable. Every effort should be made to mitigate any identified issues that effect critical business components or processes. Examples of mitigation methods include—

(1) Purchasing redundant or additional system architecture.

(2) Creating or modifying existing system operating procedures.

(3) Identifying alternate redundant locations that systems will failover to in order to reduce the impact of an initial failure.

f. Recovery strategies. Recovery strategies are specifics with regard to restoring affected system(s) or business processes to 100 percent of their full capacity before, during, or after an emergency. The first step in this process is to identify what will need to be recovered given the installations worse case scenario. For example, a catastrophic event that occurs at a critical communications center could cause the loss of off-post network connectivity for both the Secure Internet Protocol Network (SIPRNet) and Non-Secure Internet Protocol Router Network (NIPRNet). This would cause the loss of off-post e-mail services and internet connectivity. Strategies need to be created to meet each individual issue independently as well as the major issue surrounding the loss of the communications center. A good plan sees services and processes that depend on the critical communications center partially restored even though the critical communications center is down. An agreement should be put place with the locally assigned tactical unit to support SIPRNet connectivity in an emergency. The COOP site manager should have discussed emergency internet connectivity with the local data service center, developed procedures for Tier 1 and 2 help-desk support, and been assured that the required level of quality of service will be met. The location for the connection should be already identified in the contingency plan. All associated documentation and paperwork necessary to execute the recovery strategies is included in the contingency plan.

g. IT contingency plan. The IT contingency plan is often worked in concert with installation recovery strategies. As recovery strategies combine to restore connectivity following a catastrophic event, IT contingency plans are combined to restore individual systems that are necessary for the recovery strategy to work. IT contingency plans are checklists and procedures for building and recovering a particular system or service from the ground up. For example, a fire destroys the room that houses the installation mail servers and switches that connect the servers to the network.

(1) Given this scenario, the following contingency plans are executed. Each item listed below is an IT contingency plan. The entire procedure would be considered the mail recovery process:

(a) An alternate server is loaded with appropriate mail server software.

(b) A backup of the mail store from the affected server is restored from tape and integrated into the alternate server's mail store.

(c) A backup configuration from the original switch is restored to an alternate switch.

(d) Connectivity is restored and critical users are informed that their mail server is now available.

(2) The mail recovery process is not possible unless contingency team members have a—

(a) List of critical mail users.

(b) Documented mail server-build process.

(c) Process in place to backup and restore critical information stores.

(d) Call tree to assemble members of the Server and Network Recovery Teams to the scene.

(3) IT contingency plans are the basic building block for the recovery process and need to be included as part of installation contingency planning.

(4) Creating a plan and not testing it is the same as not having a plan at all. All tests conducted are planned, resourced, and supported by management. For a thorough overview of plan testing, see paragraph 3–5 of this document.

h. Maintenance of the plan. Contingency response team plans need to be continually maintained to provide support for business continuity. Administrative procedures and guidelines should be developed that provide for periodic testing and documentation maintenance of the continuity plan as well as required ongoing and needed training. The continuity plan can be maintained if changes in the business and or IT infrastructure include the initiation of reviews and updates to the plan. When any component of the contingency plan is affected, the following steps are taken:

(1) The COOP site manager is notified of the change.

(2) Effects of the change are evaluated by select contingency response team members

(3) The continuity plan is modified by the appropriate team member to reflect the change.
(4) Testing requirements are determined by the COOP site manager; if necessary, a test is scheduled.

Chapter 3
Elements of Information Technology Contingency Plans

3–1. Information technology contingency statement

An IT contingency statement is a formal organization policy that provides the authority and guidance necessary to develop an effective contingency plan.

a. The contingency plan is based on clearly defined policy, such as that found in AR 500–3, so that it is effective and ensures that personnel fully understand the organization's contingency planning requirements. The contingency planning policy statement defines the organization's overall contingency objectives and establishes the organizational framework and responsibilities for IT contingency planning.

b. To be successful, a contingency program must be supported by senior management. These officials are included in the process to develop the program policy, structure, objectives, and roles and responsibilities.

c. At a minimum, the contingency policy complies with 44 USC 3601 and AR 500–3, paragraph 1–9, which outlines minimum COOP program requirement.

d. Agencies should evaluate their IT systems, operations, and requirements to determine if additional contingency planning requirements are necessary. Key policy elements not mentioned in paragraph 2–4 of this pamphlet include—

(1) Scope as applies to the type(s) of platform(s) and organization functions subject to contingency planning.
(2) Resource requirements.
(3) Plan maintenance schedule.
(4) Frequency of backups and storage of backup media.

e. As the IT contingency policy and program are developed, they must be coordinated with related and relevant organization activities, including—

(1) IT and physical security.
(2) Human resources.
(3) IT operations.
(4) Emergency preparedness functions.
(5) Life-support services.

f. IT contingency activities should be compatible with program requirements for these areas, and contingency personnel should coordinate with representatives from each area to remain aware of new or evolving policies, programs, or capabilities.

g. Contingency plans are written in coordination with other existing plans associated with systems. Such plans include—

(1) Security-related plans, such as system security plans.
(2) Facility-level plans, such as the OEP and COOP.
(3) Organization-level plans, such as business resumption and critical infrastructure protection plans.

3–2. Business impact analysis

a. The BIA enables DOIMs to characterize fully system requirements, processes, and interdependencies and use this information to determine contingency requirements and priorities.

b. The purpose of the BIA is to correlate specific system components with the critical services that they provide and, based on that information, characterize the consequences of a disruption to the system components.

c. Results from the BIA is incorporated into the analysis and strategy development efforts for the organization's COOP, BCP, and BRP. The BIA process helps DOIMs streamline and focus their contingency plan development activities to achieve a more effective plan.

d. Critical IT resources should be identified. IT systems can be very complex, with numerous components, interfaces, and processes. A system often has multiple missions resulting in different perspectives on the importance of system services or capabilities. This first BIA step evaluates IT systems to determine the critical functions performed by the system and to identify the specific system resources required to perform them. The DOIM neds to complete two activities needed to formulate this step:

(1) Identify and coordinate with internal and external POCs associated with the system to characterize the ways that they depend on or support the IT system. When identifying contacts, it is important to include organizations that provide or receive data from the system as well as contacts supporting interconnected systems. This coordination enables the system manager to characterize the full range of support provided by the system, including security, managerial, technical, and operational requirements.

(2) Evaluate the system to link these critical services to system resources. This analysis usually identifies infrastructure requirements such as electric power, telecommunications connections, and environmental controls. Specific IT equipment, such as routers, application servers, and authentication servers are usually considered critical. However, the analysis may determine that certain IT components, such as a printer or print server, are not needed to support critical services.

e. The impacts of disruption should be identified.

(1) The effects of the outage may be tracked over time. This enables the DOIM to identify the maximum allowable time a resource may be denied before it prevents or inhibits the performance of an essential function.

(2) The effects of the outage may be tracked across related resources and dependent systems, identifying any cascading effects that may occur as a disrupted system affects other processes that rely on it.

f. Allowable outage times for critical IT resources should be identified. The DOIM determines the optimal point to recover the IT system by balancing the cost of system inoperability against the cost of resources required for restoring the system. The point where the two lines meet defines how long the organization can afford to allow the system to be disrupted.

g. Recovery priorities should be developed.

(1) The outage impact(s) and allowable outage times characterized in the previous step enable the DOIM to develop and prioritize recovery strategies that personnel should implement during contingency plan activation. For example, if the outage impacts step determines that the system should be recovered within 4 hours, the DOIM would need to adopt measures to meet that requirement. Similarly, if most system components could tolerate a 24-hour outage but a critical component could be unavailable for only 8 hours, the DOIM would prioritize the necessary resources for the critical component.

(2) By prioritizing these recovery strategies, the DOIM may make more informed, tailored decisions regarding contingency resource allocations and expenditures, saving time, effort, and costs.

h. Preventative controls for each critical IT resource should be identified.

(1) The BIA can provide the DOIM with vital information about system availability and recovery requirements. In some cases, the outage impacts identified in the BIA may be mitigated or eliminated through preventive measures that deter, detect, and/or reduce impacts to the system.

(2) Where feasible and cost-effective, preventive methods are preferable to actions that may be necessary to recover the system after a disruption. A wide variety of preventive controls are available, depending on system type and configuration; however, some common measures are listed below:

(a) Appropriately sized uninterruptible power supplies (UPS) to provide short-term backup power to all system components (including environmental and safety controls).

(b) IT design changes or technical controls useful in precluding or reducing continuity issues.

(c) Gasoline- or diesel-powered generators to provide long-term backup power.

(d) Air-conditioning systems with adequate excess capacity to accommodate failure of certain components, such as a compressor.

(e) Fire detection and suppression systems.

(f) Water sensors in the computer room ceiling and floor.

(g) Plastic tarps that may protect IT equipment from water damage.

(h) Heat-resistant and waterproof containers for backup media and vital nonelectronic records.

(i) Emergency master system shutdown switch.

(j) Offsite storage of backup media, nonelectronic records, and system documentation.

(k) Technical security controls, such as cryptographic key management and least-privilege access controls.

(l) Frequent, scheduled backups.

(3) Preventive controls are documented in the contingency plan and personnel associated with the system should be trained on how and when to use the controls. These controls must be maintained in good condition to ensure their effectiveness in an emergency.

3–3. Recovery strategies

a. Recovery strategies provide a way to restore IT operations quickly and effectively following a service disruption. The strategies address disruption impacts and allowable outage times identified in the BIA. Several alternatives must be considered when developing the strategy, including cost, allowable outage time, security, and integration with larger, organization-level contingency plans. The selected recovery strategy addresses potential impacts identified in the BIA and is integrated into the system architecture during the design and implementation phases of the system life cycle. The strategy includes a combination of methods that complement one another to provide recovery capability over the full spectrum of incidents. A wide variety of recovery approaches may be considered; the appropriate choice depends on the incident, type of system, and its operational requirements. It is important to balance the costs of the recovery with the length of time planned for it. In general, the least expensive strategies take the most time to recover, and vice versa, as depicted in figure 3–1.

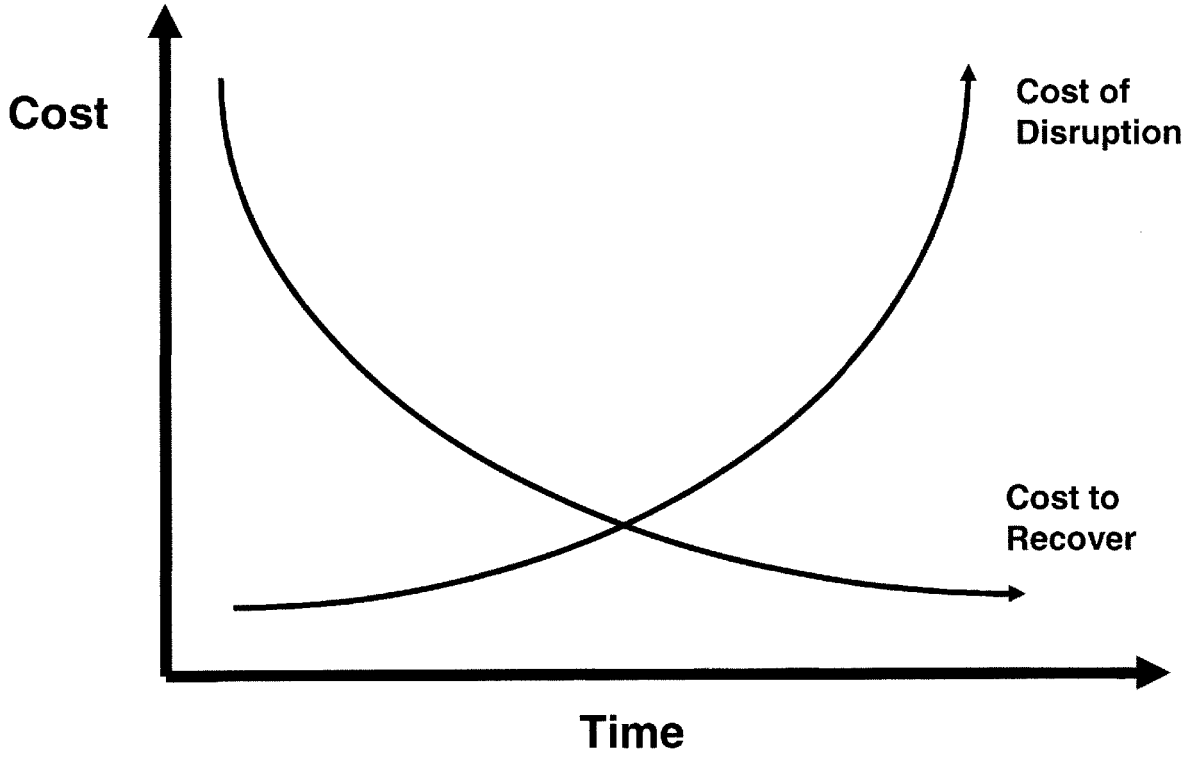


Figure 3–1. Recovery cost balancing

b. Specific recovery methods, further described in chapter 5, should be considered and may include commercial contracts with cold, warm, or hot site vendors, mobile sites, mirrored sites, reciprocal agreements with internal or external organizations, and service level agreements (SLAs) with the equipment vendors. Technologies such as Redundant Arrays of Independent Disks (RAID), automatic fail-over, UPS, and mirrored systems should be considered when developing a system recovery strategy.

(1) System data are backed up regularly. Policies specify the frequency of backups (such as daily or weekly, incremental or full), based on data criticality and the frequency that new information is introduced. Data backup policies designate the location of stored data, file-naming conventions, media rotation frequency, and method for transporting data offsite. Data may be backed up on magnetic disk, tape, or optical disks (such as compact disks). The method chosen for conducting backups is based on system and data availability and integrity requirements. These methods include electronic vaulting, mirrored disks (using direct access storage devices (DASD) or RAID), and floppy disks.

(2) It is good business practice to store backed-up data offsite. Data storage facilities are specially designed to archive media and protect data from threatening elements. If using offsite storage, data are backed up at the organization's facility and then labeled, packed, and transported to the storage facility. If the data is required for recovery or testing purposes, the organization contacts the storage facility requesting specific data to be transported to the organization or to an alternate facility. Some storage facilities offer media transportation and response and recovery services.

(3) When selecting an offsite storage facility and vendor, the following criteria may be considered:

(a) Geographic area in terms of distance from the organization and the probability of the storage site being affected by the same disaster as the organization.

(b) Accessibility in terms of the length of time necessary to retrieve the data from storage and the storage facility's operating hours.

(c) Security capabilities of the storage facility and employee confidentiality, which should meet the data's sensitivity and security requirements.

(d) Structural and environmental conditions of the storage facility (temperature, humidity, fire prevention, and power management controls).

(e) The ability to conduct tape archiving, failover, and data replication.

(f) Cost of shipping, operational fees, and disaster response/recovery services. Restoration strategies balance the cost of the approach with the priority of the system(s) being restored.

3–4. Plan testing, training, and exercise

a. As mentioned in paragraph 2–4, plan testing is a critical element of a viable contingency capability. Testing enables plan deficiencies to be identified and addressed. Testing also helps evaluate the ability of the recovery staff to implement the plan quickly and effectively. Each IT contingency plan element is tested to confirm the accuracy of individual recovery procedures and the overall effectiveness of the plan. The following areas are addressed in a contingency test:

(1) System recovery on an alternate platform from backup media.

(2) Coordination among recovery teams.

(3) Internal and external connectivity.

(4) System performance using alternate equipment.

(5) Restoration of normal operations.

(6) Notification procedures.

b. To derive the most value from the test, the DOIM or COOP site manager develops a test plan designed to test the selected element(s) against explicit test objectives and success criteria. It is recommended that the test plan include at least quarterly communications exercises with tenants and IT support elements. The use of test objectives and success criteria enables the effectiveness of each plan element and the overall plan to be assessed. The test plan may include a schedule detailing the time frames for each test and test participants. The test plan also delineates clear scope, scenario, and logistics. The scenario chosen may be a worst case incident or an incident most likely to occur. It also mimics reality as closely as possible. At the installation level, contingency response team membership is usually an extra duty. The official responsible for testing the IT contingency plan is competing for the time and resources of personnel who are not assigned to his or her direct supervision. Poorly conducted and planned testing is a waste of time and money. Poor use of personnel time in testing will erode the ability of the official responsible for testing to accomplish planning and training tasks in the future. Management support and buy in is the key. There is nothing worse than planning a training event and having a poor turnout because the need to test and train was not emphasized by the local management base. Current regulations require that continuity plan testing be conducted a minimum of once per year. The following list contains samples of the type of testing that may be conducted at the installation level:

(1) *Table top.* Contingency response team members are alerted or assembled to a location and allowed a certain quantity of time to work through a contingency scenario. This type of training is the easiest and least expensive method in which to test emergency preparedness.

(2) *System testing.* System testing entails utilizing only a portion of the contingency response team and is limited to a specific system or process. This type of testing is excellent for instituting new systems, or new procedures for old systems, into the continuity plan. System testing can also be used to test and train on failover hardware and procedures. For example, a failover test can be conducted on redundant firewall modules in a router.

(3) *Contingency rehearsal.* This is a full test of the DOIM's or the installation's ability to manage a disaster scenario. It is the most time intensive and costly type of rehearsal to conduct. This type of testing should be conducted annually. The DOIM coordinates with NETCOM or other IT support providers as required. The DOIM engages in quarterly communications exercises with supported tenants and IT support elements.

(4) *Alert and notification.* A call tree activation scenario ensures that all personnel on the contingency response team or their alternate can be contacted. This test verifies telephone and cell phone numbers as well as the ability of each contingency team element to respond when primary members cannot be contacted. The test can terminate at any point desired by the COOP site manager. For example, only the call tree can be tested or all personnel can be called up and a table top training event conducted. As has been seen in the past, significant events often overload telecommunications systems. It is important to explore alternative means of communicating, such as—

(a) Mass media.

(b) Internet.

(c) Tactical radio.

(d) Priority telephone lines

c. Upon the completion of any test, a thorough after action review is conducted with all individuals involved in the testing and training event. IT contingency plan documentation is updated and a full report filed to include lessons learned. Action items are assigned to team members and all deliverables tracked. Procedures found to be inadequate are changed and retested as soon as practically possible.

d. Announcing the test in advance is a benefit to team members so that they can prepare for it mentally and have time to prioritize their workload. It is likely that some team members may not be available because of absence or because the test may be disruptive to their workload. Personnel availability issues are beneficial to the plan to capture how a real response may play out, thus providing critical input to plan modifications. It is important that an exercise never disrupt normal operations. If testing at the alternate facility, the DOIM coordinates test dates and operations with

the facility. Test results and lessons learned are documented and reviewed by test participants and other personnel as appropriate. Information collected during the test and post-test reviews that improve plan effectiveness are incorporated into the contingency plan.

e. Training for personnel with contingency plan responsibilities complements testing. Training is provided at least annually; new hires who will have plan responsibilities receive training shortly after they are hired. Ultimately, contingency plan personnel are trained to the extent that they are able to execute their respective recovery procedures without aid of the actual document. This is an important goal in the event that paper or electronic versions of the plan are unavailable for the first few hours resulting from the extent of the disaster. Recovery personnel are trained on the following plan elements:

(1) Purpose of the plan.
(2) Cross-team coordination and communication.
(3) Reporting procedures.
(4) Security requirements.
(5) Team-specific processes (notification/activation, recovery, and reconstitution phases).
(6) Individual responsibilities (notification/activation, recovery, and reconstitution phases).
(7) Tape archiving.

3–5. Contingency plan maintenance

a. Because the IT contingency plan contains potentially sensitive operational and personnel information, its distribution is marked accordingly and controlled according to AR 380–5. Typically, copies of the plan are provided to recovery personnel for storage at home and office. A copy is also stored at the alternate site and with the backup media. Storing a copy of the plan at the alternate site ensures its availability and good condition in the event local plan copies cannot be accessed because of the disruption. The DOIM maintains a record of copies of the plan and to whom they were distributed. Other information to be stored with the plan includes contracts with vendors (SLAs and other contracts), software licenses, system users manuals, security manuals, and operating procedures.

b. Changes made to the plan, strategies, and policies should be coordinated through the DOIM, who, as part of a change management process, communicates changes to the representatives of associated plans or programs, as necessary. The DOIM records plan modifications using a Record of Changes, which lists the page number, change comment, and date of change. The Record of Changes is integrated into the plan.

c. The DOIM coordinates frequently with associated internal and external organizations and system POCs to ensure that impacts caused by changes within either organization are reflected in the contingency plan. Strict version control is maintained by requesting old plans or plan pages to be returned to the DOIM in exchange for the new plan or plan pages.

d. The DOIM references AR 380–5 for information pertaining to the protection of information stored at the site of a contingency situation. More specifically, plans should be in place to monitor emergency personnel so that classified material is accounted for as part of the damage assessment phase.

e. The DOIM also evaluates supporting information to ensure that the information is current and continues to meet system requirements adequately. This information includes the following:

(1) Alternate site contract, including testing times.
(2) Offsite storage contract.
(3) Software licenses.
(4) Memorandums of understanding (MOUs) or vendor SLAs.
(5) Hardware and software requirements.
(6) System interface agreements.
(7) Security requirements.
(8) Recovery strategy.
(9) Contingency policies.
(10) Training and awareness materials.

f. Although some changes may be quite visible, others will require additional analysis. The BIA should be reviewed periodically and updated with new information to identify new contingency requirements or priorities. As new technologies become available, preventive controls may be enhanced and recovery strategies may be modified. A sample checklist to assist in determining the viability of contingency planning elements would include columns across the top to check for policy, procedures, implementation, testing, integration, the making of a risk-based decision, comments, and the approving officials initials as well as the following "critical element" questions in rows:

(1) Have the most critical and sensitive operations and their supporting computer resources been identified?
(2) Are critical data files and operations identified and the frequency of file backup documented?
(3) Are resources supporting critical operations identified?
(4) Have processing priorities been established and approved by management?
(5) Has a comprehensive contingency plan been developed and documented?

(6) Is the plan approved by key affected parties?
(7) Are responsibilities for recovery assigned?
(8) Are there detailed instructions for restoring operations?
(9) Is there an alternate processing site; if so, is there a contract or interagency agreement in place?
(10) Is the location of stored backups identified?
(11) Are backup files (tape archives, data replications) created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are damaged?
(12) Is system and application documentation maintained at the off-site location?
(13) Are all system defaults reset after being restored from a backup?
(14) Are the backup storage site and alternate site geographically removed from the primary site and physically protected?
(15) Has the contingency plan been distributed to all appropriate personnel?
(16) Are tested contingency/disaster recovery plans in place?
(17) Is an up-to-date copy of the plan stored securely offsite?
(18) Are employees trained in their roles and responsibilities?
(19) Is the plan periodically tested and readjusted as appropriate?

Chapter 4
Contingency Operations and Emergency Procedures

There are several elements that go into successful contingency planning. Figure 4–1 provides a snapshot of these elements in regards to developing an IT contingency plan with the rest of the chapter providing more in-depth information.

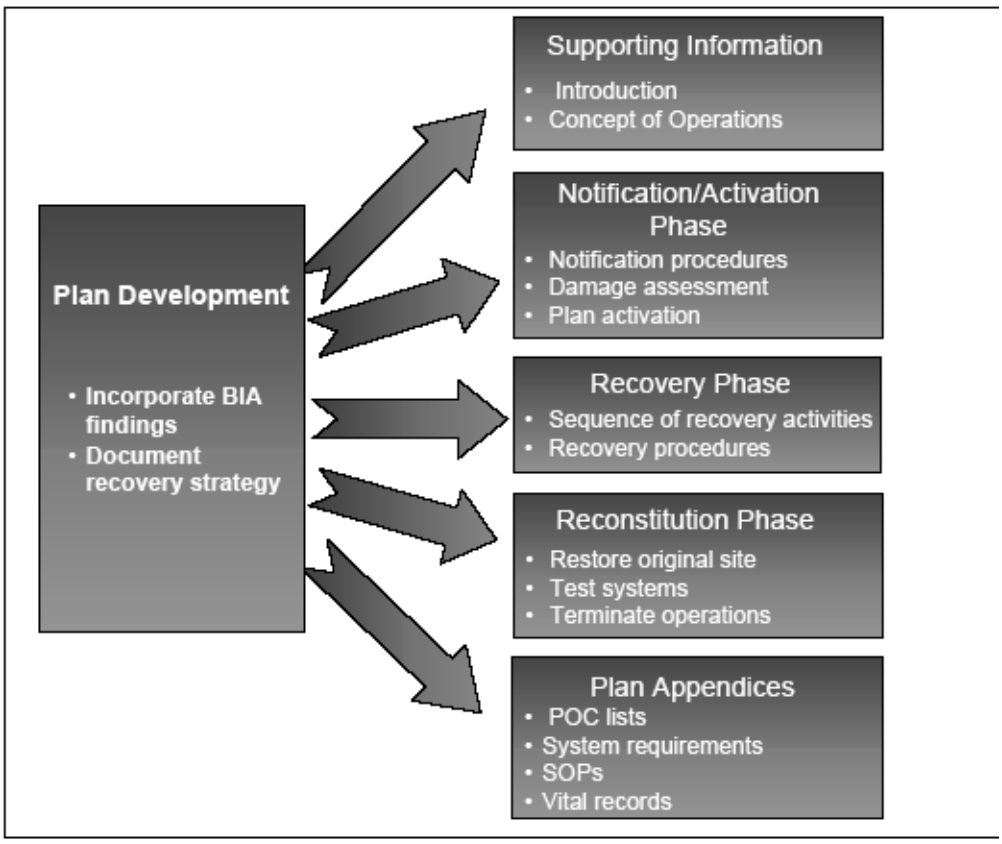


Figure 4–1. Contingency plan structure

4–1. IT contingency plan supporting information

a. The supporting information component is the responsibility of the DOIM or other IT official. This section includes an introduction and concept of operations (CONOPS) section that provides essential background or contextual information that makes the contingency plan easier to understand, implement, and maintain. These details aid in understanding the applicability of the guidance, in making decisions on how to use the plan, and in providing information on where associated plans and information outside the scope of the plan may be found. The DOIM or other responsible IT official should seek input from customers (users and tenants) for validation of the plan.

b. The introduction section orients the reader to the type and location of information contained in the plan. Generally, the section includes the purpose, applicability, scope, references/requirements, and record of changes. These subsections are—

(1) *Purpose.* This subsection establishes the reason for developing the IT contingency plan and defines the plan objectives.

(2) *Applicability.* The subsection documents the organization(s) impacted by the IT contingency plan. All related plans that support or are supported by the IT contingency plan are identified and their relationship should be described. These related plans are included as appendixes to the contingency plan.

(3) *Scope.* The scope discusses the issues, situations, and conditions addressed and not addressed in the plan. The section identifies the target system and the locations covered by the contingency plan if the system is distributed among multiple locations. For example, the plan may not address short-term disruptions expected to last fewer than 4 hours and is not likely to address the entire span of contingency needs resulting from catastrophic events that might destroy the IT facility. The scope addresses any assumptions made in the plan, such as the assumption that all key personnel would be available in an emergency. However, assumptions are not used as a substitute for thorough planning. For example, the plan should not assume that disruptions would occur only during business hours; by developing a contingency plan based on such an assumption, the contingency planning coordinator might be unable to recover the system effectively if a disruption were to occur during nonbusiness hours.

(4) *References/requirements.* This subsection identifies the Federal or organization requirement for contingency planning.

(5) *Record of changes.*

(a) The contingency plan is a living document that is changed as required to reflect system, operational, or organizational changes.

(b) Modifications made to the plan should be recorded in the record of changes located at the front of the plan.

(c) Changes to the plan are made by the contingency planning coordinator or an alternate and published in a format that should prevent unofficial or unapproved changes to the plan.

(d) Suggested column headings for a record of changes are page number, change comment, date of change, and signature of IT contingency plan coordinator.

c. The CONOPS section provides additional details about the IT system, the contingency planning framework; and response, recovery, and resumption activities. This section may include the following elements:

(1) System description. It is necessary to include a general description of the IT system covered in the contingency plan. The description includes the IT system architecture, location(s), and any other important technical considerations. A system architecture diagram, including security devices (for example, firewalls, internal and external connections) is useful. The content for the system description can usually be gleaned from the system security plan.

(2) Line of succession. The order of succession identifies personnel responsible to assume authority for executing the contingency plan in the event the designated person is unavailable or unable to do so.

(3) Responsibilities. The responsibilities section presents the overall structure of contingency response teams, including the hierarchy and coordination mechanisms and requirements among the teams. The section also provides an overview of team member roles and responsibilities in a contingency situation. Teams and team members are designated for specific response and recovery roles during contingency plan activation. Roles are assigned to team positions rather than to a specific individual. Listing team members by role rather than by name not only reduces confusion if the member is unavailable to respond but also helps reduce the number of changes that would have to be made to the document because of personnel turnover.

4–2. Emergency actions

a. Under emergency and contingency conditions, the DOIM or other IT official has the authority to take independent action necessary to maintain operational information systems. Such action might include—

(1) Exchange or substitution of commercially leased or maintained equipment.

(2) Substitution of equipment or circuitry from lower precedence to higher precedence requirements.

(3) Obligation of resources to fulfill priority commitments.

b. Independent actions taken which normally require the approval and coordination of higher headquarters prior to implementation are:

(1) Documented in the format appropriate for the information systems involved.

(2) Reported through command channels to the next-highest headquarters at the earliest opportunity.

4–3. Notification/activation phase

This phase defines the initial actions taken once a system disruption or emergency has been detected or appears to be imminent. This phase includes activities to notify recovery personnel, assess system damage, and implement the plan. At the completion of this phase, the contingency response team, explained below, should be prepared to perform contingency measures to restore system functions.

a. Contingency response team. The contingency response team is composed of the people responsible for planning and implementing the IT contingency plan. One example of a contingency response team is found in figure 4–2. Note that the contingency planning coordinator shown in figure 4–2 may have other titles. For example, the DOIM may be responsible for overall installation contingency planning while the person responsible for IT services and support should be the contingency planning coordinator for IT services and support.

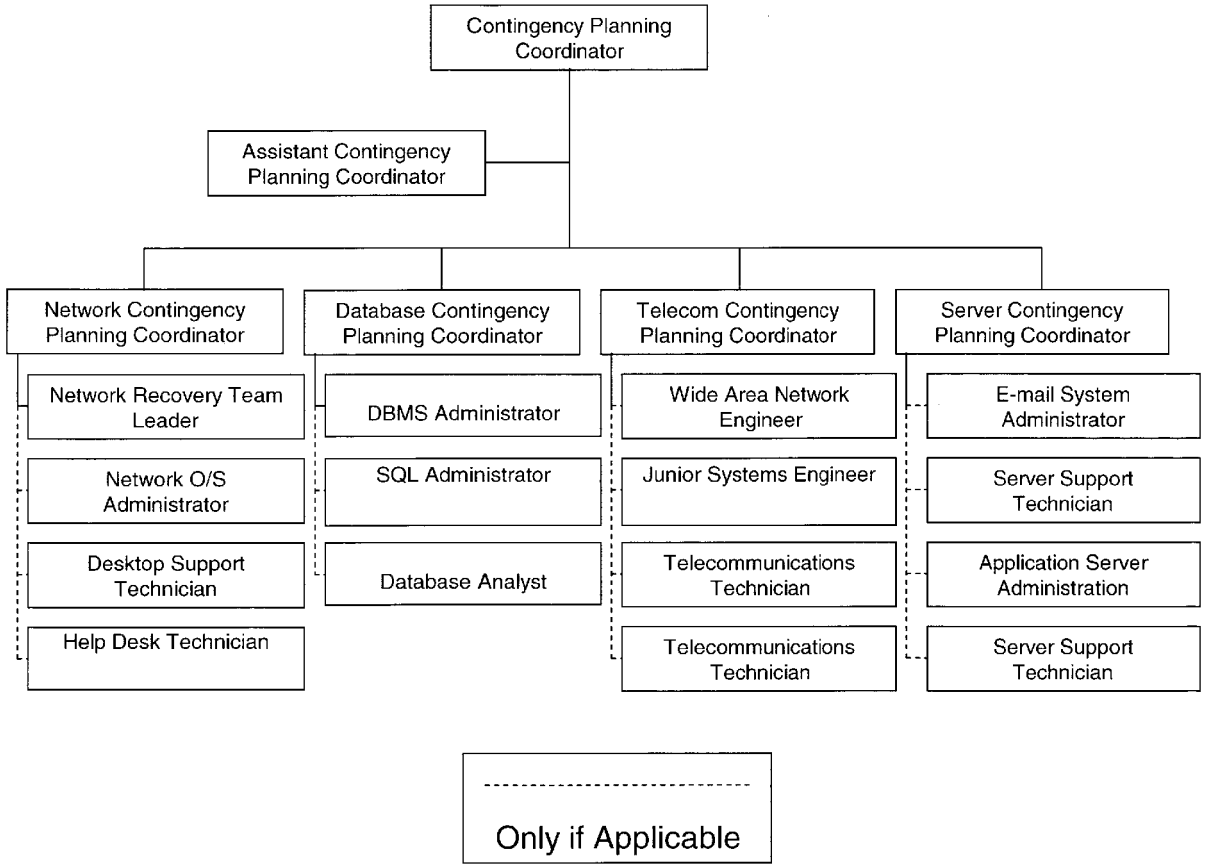


Figure 4–2. Sample call tree

b. An event occurrence with or without notice. For example, advanced notice is often given that a hurricane will affect an area or that a computer virus is expected on a certain date. However, there may be no notice of equipment failure or a criminal act. Notification procedures are documented in the plan for both situations. The procedures describe the methods used to notify recovery personnel during business and non-business hours. Prompt notification is important for reducing the effects on the IT system. In some cases, it may provide enough time to allow system personnel to shut down the system gracefully to avoid a hard crash. Following the disaster, notification is sent to the contingency response team so that it may determine the status of the situation and appropriate next steps. When damage assessment is complete, the appropriate recovery and support teams are notified.

(1) Notifications can be accomplished through a variety of methods, including phone, pager, e-mail, or cell phone. Notifications sent via e-mail are done so with caution because there is no way to ensure positive feedback. Although e-mail has potential as an effective method of disseminating notifications to work or personal accounts, there is no way to ensure that the message will be read. Work e-mail accounts often receive prolific amounts of messages resulting in personnel screening their accounts; personal e-mail accounts are often checked as infrequently as once a week or less. If using an e-mail notification method, recovery personnel are informed of the necessity to frequently and regularly check their accounts. Notifications sent during business hours are sent to the work address, whereas personal e-mail messaging may be useful in the event that the LAN is down. Notification tools that are effective during widespread disasters are radio and television announcements and Web sites.

(2) The notification strategy defines procedures to be followed in the event that specific personnel cannot be contacted. Notification procedures are documented clearly in the contingency plan. A common notification method is a call tree. This technique involves assigning notification duties to specific individuals, who in turn are responsible for notifying other recovery personnel. The call tree accounts for primary and alternate contact methods and should discuss procedures to be followed if an individual cannot be contacted. A sample call tree is found in figure 4–2.

(3) Personnel to be notified must be clearly identified in the contact lists appended to the plan. This list identifies personnel by their team position, name, and contact information (for example, home, work, and pager numbers, e-mail addresses, and home addresses).

(4) Notifications are also sent to POCs of external organizations or interconnected system partners that may be adversely affected if they are unaware of the situation. Dependent on the type of disruption, the POC may have recovery responsibilities. Therefore, for each system interconnection with an external organization, a POC is identified to the extent that the organizations will assist each other and the terms under which the assistance, in accordance with the system interconnection agreement, will be provided. These POCs are listed in an appendix to the plan.

(5) The type of information to be relayed to those being notified is documented in the plan. To determine how the contingency plan will be implemented following an emergency, it is essential to assess the nature and extent of the damage to the system. This damage assessment is completed as quickly as the given conditions permit, with personnel safety remaining the highest priority. Therefore, when possible, the contingency response team is the first team notified of the incident. The amount and detail of information relayed may depend on the specific team being notified. As necessary, notification information may include the following:

(a) Nature of the emergency that has occurred or is impending.

(b) Cause of the emergency or disruption.

(c) Area affected by the emergency.

(d) Potential for additional disruptions or damage.

(e) Loss of life or injuries.

(f) Inventory and functional status of IT equipment (for example, fully functional, partially functional, and nonfunctional).

(g) Type of damage to IT equipment or data (for example, water damage, fire and heat, physical impact, and electrical surge).

(h) Status of physical infrastructure (for example, structural integrity of computer room, condition of electric power, telecommunications, and heating, ventilation, and air-conditioning).

(i) Items to be replaced (for example, hardware, software, firmware, and supporting materials).

(j) Response and recovery details.

(k) Where and when to convene for briefing or further response instructions.

(l) Estimated time to restore normal services.

(m) Instructions to prepare for relocation for estimated time period.

(n) Instructions to complete notifications using the call tree (if applicable).

c. Damage assessment responsibilities. Personnel with damage assessment responsibilities must understand and be able to perform these procedures in the event the paper plan is unavailable during the situation. Once the impact to the

system has been determined, the appropriate teams are notified of updated information and planned response to the situation.

d. Plan activation. The IT contingency plan is activated only when the damage assessment indicates that one or more of the activation criteria for that system is met. If an activation criterion is met, the contingency planning coordinator or senior information management official (as appropriate) should activate the plan. Activation criteria for events are unique for each organization and should be stated in the contingency planning policy statement. Criteria may be based on—

(1) Safety of personnel and/or extent of damage to the facility.

(2) Extent of damage to system (for example, physical, operational, or cost).

(3) Criticality of the system to the organization's mission (for example, critical infrastructure protection asset).

(4) Anticipated duration of disruption.

e. Recovery strategy selection. Once the system damage has been characterized, the contingency planning coordinator may select the appropriate recovery strategy.

4–4. Recovery phase

Recovery operations begin after the damage assessment has been completed (if possible), the contingency plan has been activated, personnel have been notified, and appropriate teams have been mobilized. Recovery phase activities focus on contingency measures to execute temporary IT processing capabilities, repair damage to the original system, and restore operational capabilities at the original or new facility. At the completion of the recovery phase, the IT system should be operational and performing the functions designated in the plan. Depending on the recovery strategies defined in the plan, these functions could include temporary manual processing, recovery and operation on an alternate system, or relocation and recovery at an alternate site. Teams with recovery responsibilities must understand and be able to perform these recovery strategies well enough that if the paper plan is unavailable during the initial stages of the event, they can still perform the necessary activities.

a. It is essential that contingency plan coordinators plan and budget for the strategies they plan to use to deal with a crisis. A sample recovery strategy budget planning template is provided at table 4–2.

Table 4–2
Sample recovery budget plan

Budget planning considerations	Vendor costs	Hardware costs	Software costs	Travel/shipping costs	Labor/contractor costs	Testing costs	Supply costs	Totals
Cold site	$25,000	$30,000	$3,000	$15,000	$20,000	$2,000	$10,000	**$105,000**
Warm site	$50,000	$40,000	$4,000	$10,000	$15,000	$3,000	$8,000	**$130,000**
Hot site	$75,000	$45,000	$4,500	$5,000	$10,000	$4,000	$5,000	**$148,500**
Mobile site	$75,000	$45,000	$4,500	$8,000	$15,000	$4,000	$5,000	**$156,500**
Mirrored site	$50,000	$40,000	$4,000	$5,000	$10,000	$3,000	$3,000	**$115,000**
Commercial	$100,000	0	0	$5,000	$10,000	$4,000	$3,000	**$122,000**
Internal	$25,000	$30,000	$3,000	0	0	$2000	$2,000	**$62,000**
SLAs	$25,000	$30,000	$15,000	0	$10,000	$3,000	0	**$83,000**
Storage	$20,000	$20,000	$5,000	0	0	0	0	**$45,000**
Existing use	0	$50,000	$3,000	$3,000	0	$2,000	$2,000	**$60,000**

b. When recovering a complex system, such as a wide area network (WAN) involving multiple independent components, recovery procedures must reflect system priorities identified in the BIA. The sequence of activities reflect the system's allowable outage time to avoid significant impacts to related systems and their application. Procedures are written in a stepwise, sequential format so system components may be restored in a logical manner. For example, if a local area network (LAN) is being recovered after a disruption, the most critical servers should be recovered before other, less critical devices, such as printers. Similarly, to recover an application server, procedures first should address

operating system restoration and verification before the application and its data are recovered. The procedures also include instructions to coordinate with other teams when certain situations occur, such as—

(1) An action is not completed within the expected time frame.

(2) A key step has been completed.

(3) Item(s) should be procured.

(4) Other system-specific concerns.

c. If conditions require the system to be recovered at an alternate site, certain materials will need to be transferred or procured. These items may include shipment of data backup media from offsite storage, hardware, copies of the recovery plan, and software programs. Procedures designate the appropriate team or team members to coordinate shipment of equipment, data, and vital records. References to applicable appendices, such as equipment lists or vendor contact information, are made in the plan where necessary. Procedures clearly describe requirements to package, transport, and purchase materials required to recover the system.

d. To facilitate recovery phase operations, the contingency plan provides detailed procedures to restore the IT system or system components. Given the extensive variety of system types, configurations, and applications, this planning guide does not provide specific recovery procedures. Procedures are assigned to the appropriate recovery team and typically address the following actions:

(1) Obtaining authorization to access damaged facilities and/or geographic area.

(2) Notifying internal and external business partners associated with the system.

(3) Obtaining necessary office supplies and work space.

(4) Obtaining and installing necessary hardware components such as computers and related peripherals.

(5) Obtaining and loading backup media.

(6) Restoring critical operating system and application software.

(7) Restoring system data.

(8) Testing system functionality including security controls.

(9) Connecting system to network or other external systems.

(10) Operating alternate equipment successfully.

e. Recovery procedures are written in a straightforward, step-by-step style. To prevent difficulty or confusion in an emergency, no procedural steps should be assumed or omitted. A checklist format is useful for documenting the sequential recovery procedures and for troubleshooting problems if the system cannot be recovered properly. The example provided in Figure 4–3 provides a subset of a procedural checklist for a LAN Recovery Team. It is suggested that the person using the checklist note the times that each step is completed.

RECOVERY PROCESS FOR THE LAN RECOVERY TEAM

These procedures are used for recovering a file from backup tapes. The LAN Recovery Team is responsible for reloading all critical files necessary to continue production.

1. Identify file and date from which file is to be recovered.
2. Identify tape number using tape log book.
3. If tape is not in tape library, request tape from recovery facility; fill out with appropriate authorizing signature.
4. When tape is received, log date and time.
5. Place tape into drive and begin recovery process.
6. When file is recovered, notify LAN Recovery Team leader.

Figure 4–3. Sample LAN recovery team checklist

4–5. Reconstitution phase

a. In the reconstitution phase, recovery activities are terminated and normal operations are transferred back to the organization's facility. If the original facility is unrecoverable, the activities in this phase can also be applied to preparing a new facility to support system processing requirements. Once the original or new site is restored to the level that it can support the IT system and its normal processes, the system may be transitioned back to the original or to the new site. Until the primary system is restored and tested, the contingency system continues to be operated. The reconstitution phase specifies teams responsible for restoring or replacing both the site and the IT system. The following major activities occur in this phase:

(1) Ensuring adequate infrastructure support, such as electric power, water, telecommunications, security, environmental controls, office equipment, and supplies.

(2) Installing system hardware, software, and firmware. This activity includes detailed restoration procedures similar to those followed in the recovery phase.

(3) Establishing connectivity and interfaces with network components and external systems.

(4) Testing system operations to ensure full functionality.

(5) Backing up operational data on the contingency system and uploading to restored system.

(6) Shutting down the contingency system.

(7) Terminating contingency operations.

(8) Securing, removing, and/or relocating all sensitive materials at the contingency site.

(9) Arranging for recovery personnel to return to the original facility.

b. These teams must understand and be able to perform their required functions without a paper plan in the event such documentation is unavailable.

4–6. Plan appendixes

Contingency plan appendices provide key details not contained in the main body of the plan. The appendices reflect the specific technical, operational, and management contingency requirements of the given system; however, some appendixes are frequently found within the IT contingency plans. Common contingency plan appendices include the following:

a. Contact information for contingency planning team personnel.

b. Vendor contact information, including offsite storage and alternate-site POCs.

c. Standard operating procedures and checklists for system recovery or processes.

d. Equipment and system requirements lists of the hardware, software, firmware, and other resources required to support system operations. Details are provided for each entry, including model or version number, specifications, and quantity.

e. Vendor SLAs, reciprocal agreements with other organizations, and other vital records.

f. Description of, and directions to, the alternate site.

g. The BIA, conducted during the planning phases, which contains valuable information about the interrelationships, risks, prioritization, and impacts to each element of the system. The BIA is included as an appendix for reference should the plan be activated.

Chapter 5
Contingency Planning for IT Systems

This section complements the process and framework guidelines presented in earlier sections by discussing technical contingency planning considerations for specific types of IT systems. The information presented in this section assists the reader in selecting, developing, and implementing specific technical contingency strategies based on the type of IT system. Because each system is unique, information is provided at a level that may be used by the widest audience. All of the information presented may not apply to a specific IT system; therefore, the contingency planning coordinator draws on information as appropriate and modifies it to meet the system's particular contingency requirements. For each IT platform type, technical measures, such as configuration management, are considered from two perspectives. First, the document discusses technical requirements or factors that the contingency planning coordinator may consider when planning a system recovery strategy. Second, technology-based solutions are provided for each platform. The technical considerations and solutions addressed in this section include preventive and recovery measures. Several of these contingency measures are common to all IT systems.

5–1. Desktop computers and portable systems

A desktop computer or portable system (for example, laptop or handheld device) typically consists of a central

processing unit, memory, disk storage, and various input and output devices. A personal computer (PC) is designed for use by one person at a time. PCs are ubiquitous in most organizations' IT infrastructures. Because the desktop and portable computers are the most common platform for routine automated processes, they are important elements in a contingency plan. PCs can be physically connected to an organization's LAN, can dial into the organization's network from a remote location, or can act as a stand-alone system. Figure 5–1 provides an overview of contingency strategies for desktop computers and portable systems.

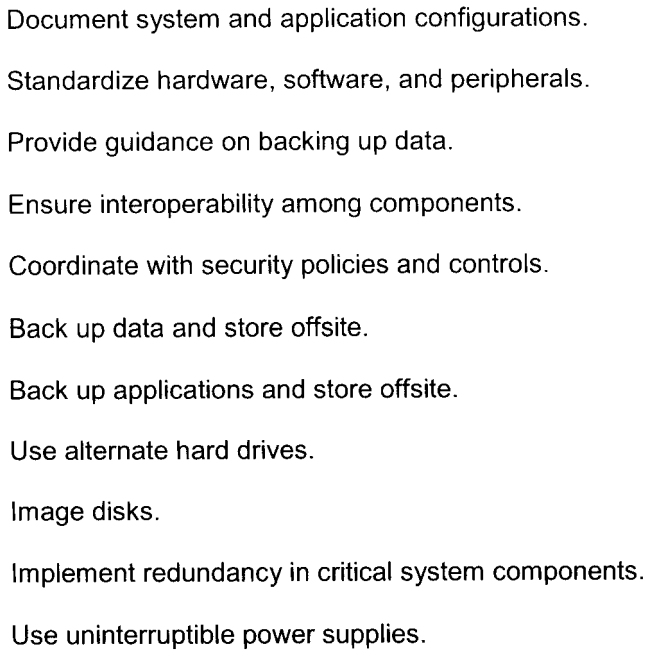


Figure 5–1. Contingency strategies for desktop computers and portable systems

a. Contingency considerations for desktop and portable systems emphasize data availability, confidentiality, and integrity. To address these requirements, the systems manager considers each of the following practices:

(1) Store backups offsite. Backup media should be stored offsite in a secure, environmentally controlled facility. If users back up data on a stand-alone system rather than saving data to the network, a means must be provided for storing the media at an alternate site. A copy of the contingency plan, software licenses, vendor SLAs and contracts, and other important documents is stored with the backup media. The BIA conducted by the contingency planning coordinator helps to ascertain how often to send backups offsite.

(2) Encourage individuals to back up data. If the PC backup process is not automated from the network, users are encouraged to back up data regularly. This task can be conducted through employee security training and awareness.

(3) Provide guidance on saving data on PCs. Instructing users to save data to a particular network folder eases the IT department's desktop support requirements. If a machine is rebuilt, the technician then knows which folders to copy and preserve while the system is being reloaded.

(4) Configuration management. Good configuration management practices are a necessary driver for good IT contingency planning. Knowing what equipment, software loads, versions, patch status, and configuration parameters are key elements of configuration management that are directs inputs into IT contingency planning. System recovery is faster if hardware, software, and peripherals are standardized throughout the organization. If standard configurations are not possible throughout the organization, then configurations are standardized by department or by machine type or model if possible. Additionally, critical hardware components that would need to be recovered immediately in the event of a disaster should be compatible with off-the-shelf computer components. This compatibility avoids delays in ordering custom-built equipment from a vendor. For more information on configuration management, refer to of Department of the Army (DA) Pamphlet (Pam) 25–1–1, paragraph 4–5.

(5) Document system configurations and vendor information. Well-documented system configurations ease recovery. Similarly, vendor names and emergency contact information should be listed in the contingency plan so that replacement equipment may be purchased quickly.

(6) Coordinate with security policies and system security controls. Desktop and portable computer contingency solutions described below should be coordinated with security policies and system security controls. Therefore, in choosing the appropriate technical contingency solution(s), similar security controls and security-related activities (for example, risk assessment, vulnerability scanning) in the production systems is implemented in the contingency solution(s) to ensure that, during a system disruption or emergency, executing the technical contingency solution(s) does not compromise or disclose sensitive data.

(7) Use results from the BIA. Impacts and priorities discovered through the BIA of associated major applications and general support systems is reviewed to determine related requirement.

b. Contingency solutions. Wide ranges of technical contingency solutions are available for desktop computers. Several efficient practices are discussed here. Data from the BIA of major applications and general support systems are used to determine the recovery requirements and priorities to implement. Backups are the most common means to ensure data availability on PCs. The following factors must be considered when choosing the appropriate backup solution:

(1) *Equipment interoperability.* To facilitate recovery, the backup device must be compatible with platform operating system and applications and be easy to install onto different models or types of PCs.

(2) *Storage volume.* To ensure adequate storage, the amount of data to be backed up determines the appropriate backup solution.

(3) *Media life.* Each type of media has a different use and storage life beyond which the media cannot be relied on for effective data recovery.

(4) *Backup software.* When choosing the appropriate backup solution, the software or method used to back up data must be considered. The encryption of backup media is considered as a means of thwarting data theft. In some cases, the backup application can be as simple as a file copy using the operating system file manager; in cases involving larger data transfers, a third-party application may be needed to automate and schedule the file backup. PC data backups can be accomplished in various ways, including those listed below:

(a) Floppy diskettes. Floppy diskette drives come standard with many desktop computers and represent the cheapest backup solution; however, these drives have a low storage capacity and are slow.

(b) Removable cartridges. Removable cartridges are not common in desktop computers and are often offered as a backup solution as a portable or external device. Removable cartridges (jump drives) are more expensive than floppy diskettes and are comparable in cost to tape media depending on the media model and make. However, removable cartridges are fast, and their portability allows for flexibility. The portable devices come with special drivers and application to facilitate data backups.

(c) Compact disc(CD)/digital video disc (DVD). CD/DVD and CD read-only memory (CD–ROM) drives come standard in most desktop computers; however, not all computers are equipped with writable CD drives. CDs are low-cost storage media and have a higher storage capacity than floppy diskettes. To read from a CD, the operating system's file manager is sufficient; however, to write to a CD/DVD, a rewritable CD/DVD drive and the appropriate software are required.

(d) Network storage. Data stored on networked PCs can be backed up to a networked disk or a networked storage device.

(e) Networked disk. A server with data storage capacity is a networked disk. The amount of data that can be backed up from a PC is limited by the network disk storage capacity or disk allocation to the particular user. However, if users are instructed to save files to a networked disk, the networked disk itself should be backed up through the network or server backup program.

(f) Networked storage device. A network backup system can be configured to back up the local drives on networked PCs. The backup can be started from either the networked backup system or the actual PC.

(g) Replication or synchronization. Data replication or synchronization is a common backup method for portable computers. Handheld computers or laptops may be connected to a PC and replicate the desired data from the portable system to the desktop computer.

(h) Internet backup. Internet backup or online backup is a commercial service that allows PC users to back up data to a remote location over the Internet for a fee. A utility is installed onto the PC that allows the user to schedule backups, select files and folders to be backed up, and establish an "archiving" scheme to prevent files from being overwritten. Data can be encrypted for transmission; however, this impedes the data transfer speed over a modem connection. The advantage of internet backup is that the user is not required to purchase data backup hardware or media.

c. In addition to backing up data, organizations must also back up system drivers. Organizations should store software and software licenses in a secondary location. If the software is commercial off-the-shelf (COTS), it can be purchased through a vendor if the copy or license installed before the destruction is unavailable. However, at a minimum, custom-built applications installed on desktops are saved and stored at an alternate location or backed up through one of the methods described above. Instructions on recovering custom-built applications at an alternate site also should be documented, particularly if the application has hard-coded drive mappings (for the PC or network server). Code that prevents the application from running on a different system should be discouraged. If driver

mappings are hard coded, the application should be modified to enable the application to be restored on another system other than the original.

d. The popularity of encryption as a security tool used on portable computers is growing. With increased use of digital signatures for nonrepudiation and the use of encryption for confidentiality, organizations may consider including encryption key pairs in their backup strategy. If the encryption key pair and verification key are stored on the PC, data can become unrecoverable or unverifiable if the PC becomes corrupted.

e. Because portable computers are vulnerable to theft, encryption can be used to protect data from being disclosed on a stolen computer. Portable computer users can also be provided a second hard drive to be used while on travel. The second hard drive contains only the minimum applications and data necessary. By using a second hard drive, if the laptop is stolen, the amount of data loss is minimized.

f. Imaging represents another contingency solution. A standard desktop computer image can be stored, and the corrupted computer can be reloaded. Imaging installs the applications and setting stored in the image; however, all data currently on the disk will be lost. Therefore, PC users should be encouraged to back up their data files. Because disk images can be large, dedicated storage, such as a server or server partition, may need to be allocated for the disk images alone. Software may be needed to push the images across the network. To decrease the number of images necessary for recovery in the event that multiple PCs are corrupted, standardizing PC models and configurations across all organizations (configuration management) saves space and eases the process of rebuilding computers. If site relocation is necessary, PC configurations and basic applications needed for mission-critical processing should be documented in the contingency plan.

5–2. Servers

Servers support file sharing and storage, data processing, central application hosting (such as e-mail or a central database), printing, access control, user authentication, remote access connectivity, and other shared network services. Local users log into the server through networked PCs to access resources that the server provides. Figure 5–2 provides an overview of contingency strategies for servers.

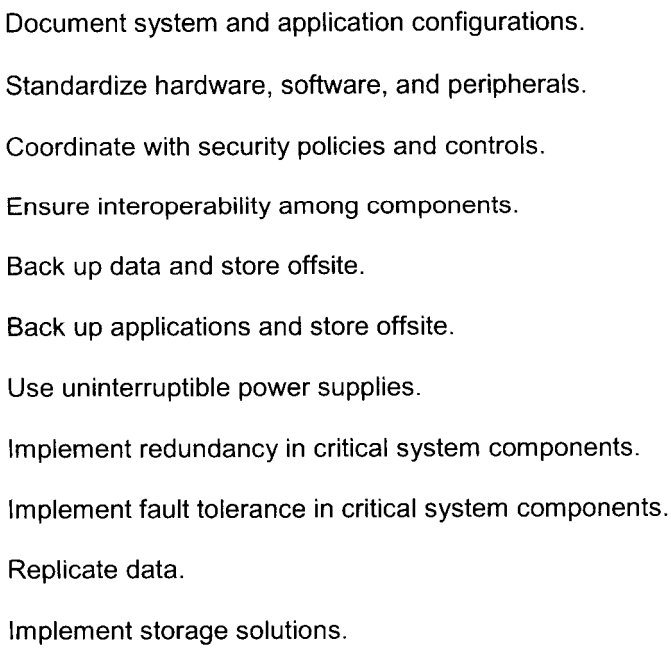


Figure 5–2. Server contingency strategies

a. Because servers can support or host numerous critical applications, server loss could cause significant problems to business processes.

(1) *Store backup media and software offsite.* As described previously, backup media and software is stored offsite in a secure, environmentally controlled facility. The storage facility should be located far enough away from the original site to reduce the likelihood that both sites would be affected by the same event.

(2) *Standardize hardware, software, and peripherals.* System recovery may be expedited if hardware, software, and peripherals are standardized throughout the organization or site. Standard configurations is documented in the contingency plan.

(3) *Document system configurations and vendors.* Maintaining detailed records of system configurations enhances system recovery capabilities. Additionally, vendors that supply essential hardware, software, and other components should be identified in the contingency plan.

(4) *Coordinate with security policies and system security controls.* Server contingency solutions are coordinated with security policies and system security controls. Thus, in choosing the appropriate technical contingency solution(s), similar security controls and security-related activities (for example, risk assessment, vulnerability scanning) in the production environment should be implemented in the contingency solution(s) to ensure that, during a system disruption or emergency, executing the technical contingency solution(s) does not compromise or disclose sensitive data.

(5) *Use results from the BIA.* Impacts and priorities discovered through the BIA of associated major applications and general support systems are reviewed to determine related requirements.

b. Several technical measures are available to enhance server recovery capabilities. The BIA of major applications and general support systems provide information to assist in determining the recovery requirements and priorities. Server contingency planning emphasizes reliability and availability of the network services provided by the server. When selecting the appropriate technical contingency solution, data confidentiality and sensitivity requirements are also considered. Additionally, when selecting the appropriate server contingency solution, the availability requirements for the server, its applications, and data are assessed. As a preventive contingency measure, critical functions are not co-located on servers with noncritical functions if possible. For example, a server hosting a critical application is dedicated to that application and not providing other resources. As with PCs, servers are backed up regularly. Servers can be backed up through a distributed system, in which each server has its own drive, or through a centralized system, where a centralized backup device is attached to one server. Three types of system backup methods are available to preserve server data:

(1) *Full.* A full backup captures all files on the disk or within the folder selected for backup. Because all backed-up files were recorded to a single media or media set, locating a particular file or group of files is simple. However, the time required to perform a full backup can be lengthy. In addition, full backups of files that do not change frequently (such as system files) could lead to excessive, unnecessary media storage requirements.

(2) *Incremental.* An incremental backup captures files that were created or changed since the last backup, regardless of backup type. Incremental backups afford more efficient use of storage media, and backup times are reduced. However, to recover a system from an incremental backup, media from different backup operations may be required. For example, consider a case in which a directory needed to be recovered. If the last full backup was performed three days prior and one file had changed each day, then the media for the full backup and for each day's incremental backups would be needed to restore the entire directory.

(3) *Differential.* A differential backup stores files that were created or modified since the last full backup. Therefore, if a file is changed after the previous full backup, a differential backup saves the file each time until the next full backup is completed. The differential backup takes less time to complete than a full backup. Restoring from a differential backup may require less media than an incremental backup because only the full backup media and the last differential media would be needed. As a disadvantage, differential backups take longer to complete than incremental backups because the amount of data since the last full backup increases each day until the next full backup is executed.

c. A combination of backup operations can be used depending on the system configuration and recovery requirements. For example, a full backup can be conducted on the weekend with differential backups conducted each evening. In developing the server backup schedule, the following questions may be considered:

(1) Where will media be stored?

(2) What data should be backed up?

(3) How frequent are backups conducted?

(4) How quickly are the backups to be retrieved in the event of an emergency?

(5) Who is authorized to retrieve the media?

(6) How long will it take to retrieve the media?

(7) Where will the media be delivered?

(8) Who will restore the data from the media?

(9) What is the media-labeling scheme?

(10) How long will the backup media be retained?

(11) When the media are stored on-site, what environmental controls are provided to preserve the media?

(12) What is the appropriate backup media?

(13) What types of media readers are used at the alternate site?

d. Backup media is stored offsite in a secure, environmentally controlled location. When selecting the offsite location, hours of the location, ease of accessibility to backup media, physical storage limitations, and the contract terms are to be taken into account. It is important that media be retrieved on a regular basis from offsite storage and tested to ensure that the backups are being performed correctly. The contingency planning coordinator references the BIA to assist in determining how often backup media are to be tested. Each backup tape, cartridge, or disk is uniquely labeled to ensure that the required data can be identified quickly in an emergency. This requires that the agency develop an effective marking and tracking strategy. One method might be to label the media by month, day, and the year that the backup was created. Other strategies can be more complex, involving multiple sets of media that are rotated as old data are either appended to or overwritten. The marking strategy must be consistent with the media retention guidelines that dictate how long the media are to be stored before they are destroyed.

e. Though offsite storage of backup media enables the system to be recovered, data added to or modified on the server since the previous backup could be lost during a disruption. To avoid this potential data loss, a backup strategy may need to be complemented by redundancy solutions, such as disk mirroring, RAID, and load balancing. These solutions are discussed below. Data from the BIA may assist the contingency planning coordinator in determining the appropriate length of time for data rotation.

f. RAID provides disk redundancy and fault tolerance for data storage and decreases mean time between failures. RAID is used to mask disk drive and disk controller failures. In addition, RAID increases performance and reliability by spreading data storage across multiple disk drives, rather than a single disk. RAID can be implemented through hardware or software; in either case, the solution appears to the operating system as a single logical hard drive. With a RAID system, hot swappable drives can be used-that is, disk drives can be swapped without shutting down the system when a disk drive fails. RAID technology uses three data redundancy techniques:

(1) *Mirroring.* With this technique, the system writes the data simultaneously to separate hard drives or drive arrays. The advantages of mirroring are minimal downtime, simple data recovery, and increased performance in reading from the disk. If one hard drive or disk array fails, the system can operate from the working hard drive or disk array, or the system can use one disk to process a read request and another disk for a different processing request. The disadvantage of mirroring is that both drives or disk arrays are processing in the writing-to-disks function, which can hinder system performance. Mirroring has a high fault tolerance and can be implemented through a hardware RAID controller or through the operating system.

(2) *Parity.* Parity refers to a technique of determining whether data have been lost or overwritten. Parity has a lower fault tolerance than mirroring. The advantage of parity is that data can be protected without having to store a copy of the data, as is required with mirroring.

(3) *Striping.* Striping improves the performance of the hardware array controller by distributing data across all the drives. In striping, a data element is broken into multiple pieces, and a piece is distributed to each hard drive. Data transfer performance is increased using striping because the drives may access each data piece simultaneously. Striping can be implemented in bytes or blocks. Byte-level striping breaks the data into bytes and stores the bytes sequentially across the hard drives. Block-level striping breaks the data into a given-size block, and each block is distributed to a disk.

g. RAID solutions rely on mirroring, parity, and striping techniques. Currently, 10 RAID levels are available, with each level providing a different configuration. RAID–1 and RAID–6 are the most popular levels for data redundancy and are addressed here.

(1) RAID–0 is the simplest RAID level, relying solely on striping. RAID–0 has a higher performance in read/write speeds than the other levels, but it does not provide data redundancy. Thus, RAID–0 is not recommended as a data recovery solution.

(2) RAID–1 uses mirroring to create and store identical copies on two drives. RAID–1 is simple and inexpensive to implement; however, 50 percent of storage space is lost because of data duplication.

(3) RAID–2 uses bit-level striping; however, the solution is not often employed because the RAID controller is expensive and difficult to implement.

(4) RAID–3 uses byte-level striping with dedicated parity. RAID–3 is an effective solution for applications handling large files; however, fault tolerance for the parity information is not provided because that parity data is stored on one drive.

(5) RAID–4 is similar to RAID–3, but it uses block-level rather than byte-level striping. The advantage of this technique is that the block size can be changed to meet the application's needs. With RAID–4, the storage space of one disk drive is lost.

(6) RAID–5 uses block-level striping and distributed parity. This solution removes the bottleneck caused by saving parity data to a single disk in RAID–3 and RAID–4. In RAID–5, parity is written across all drives along with the data. Separating the parity information block from the actual data block provides fault tolerance. If one drive fails, the data

from the failed drive can be rebuilt from the data stored on the other drives in the array. Additionally, the stripe set can be changed to fit the application's needs. With RAID–5, the storage space of one disk drive is lost.

h. RAID is an effective strategy for disk redundancy. However, redundancy for other critical server parts, such as the power supply, also should be provided. The server may be equipped with two power supplies, so that the second power supply may continue to support the server if the main power supply becomes overheated or unusable.

i. Although a second power supply can protect against hardware failure, it is not an effective preventive measure against power failure. To ensure short-term power and to protect against power fluctuations, a UPS should be installed. The UPS often provides enough backup power to enable the system to shut down gracefully. If high availability is required, consider the use of fuel cells or a gas/diesel-powered generator. The generator or fuel cell can be wired directly into the site's power system and can be configured to start automatically when a power interruption is detected.

j. Electronic vaulting and remote journaling are similar technologies that provide additional data backup capabilities, with backups made to remote tape drives over communication links. Remote journaling and electronic vaulting enable shorter recovery times and reduced data loss should the server be damaged between backups. Depending on the volume and frequency of the data transmissions, remote journaling or electronic vaulting could be conducted over a connection with limited bandwidth.

(1) With remote journaling, transaction logs or journals are transmitted to a remote location. If the server needed to be recovered, the logs or journals could be used to recover transactions, applications, or database changes that occurred after the last server backup. Remote journaling can either be conducted through batches or be communicated continuously using buffering software.

(2) With electronic vaulting, the system is connected to an electronic vaulting provider to allow backups to be created offsite automatically. The electronic vault could use optical disks, magnetic disks, mass storage devices, or an automated tape library as the storage devices. With this technology, data are transmitted to the electronic vault as changes occur on the servers between regular backups. These transmissions between backups are sometimes referred to as electronic journaling.

k. Server load balancing increases server and application availability. Through load balancing, traffic can be distributed dynamically across groups of servers running a common application so that no one server is overwhelmed. With this technique, a group of servers appears as a single server to the network. Load balancing systems monitor each server to determine the best path to route traffic to increase performance and availability so that one server is not overwhelmed with traffic. Load balancing can be implemented among servers within a site or among servers in different sites. Using load balancing among different sites can enable the application to continue to operate as long as one or more sites remain operational. Thus, load balancing could be a viable contingency measure depending on system availability requirements.

l. With disk replication, recovery windows are minimized because data is written to two different disks to ensure that two valid copies of the data are always available. The two disks are called the protected server (the main server) and the replicating server (the backup server). Disk replication can be implemented locally or between different locations. Two different data replication techniques are available, and each provides different recovery time objectives (RTOs) and recovery point objectives (RPOs). An RTO is the maximum acceptable length of time that elapses before the unavailability of the system severely affects the organization. The RPO is the point in time in which data should be restored in order to resume processing. Disk replication techniques include:

(1) Synchronous and mirroring methods use a disk-to-disk copy and maintains a replica of the database or file system by applying changes to the replicating server at the same time changes are applied to the protected server. The synchronous mode can degrade performance on the protected server and should be implemented only over short physical distances where bandwidth does not restrict data transfers between servers. With synchronous mirroring, the RTO can be minutes to several hours, and the RPO may be reduced to the loss of uncommitted work. Mirroring should be used for critical applications that can accept little or no data loss.

(2) Asynchronous and shadowing technique maintain a replica of the database or file system by continuously capturing changes to a log and applying the changes in the log to the replicating server. With asynchronous shadowing, the RTO can range from hours to a day, depending on the time that is required to implement the changes in the unapplied logs. An acceptable RPO is the last data transfer the shadowing server received. Asynchronous replication is useful over smaller bandwidth connections and longer distances where network latency could occur. As a result, shadowing helps to preserve the protected server's performance.

m. Replication solutions also can be operating system-dependent, called host-based replication, and can use both synchronous and asynchronous replication. To choose the appropriate disk replication technique and product, the contingency planning coordinator should evaluate platform support, integration with other complementary products, cost, speed of deployment, performance impact, and product completeness and manageability.

n. Disk replication also can act as a load balancer, where traffic is directed to the server with the most resources available. With disk replication, the protected server sends status messages to the replicating server. If the protected server stops replicating or sends a "distress" call, the replicating machine automatically assumes the protected server's functions. If the replication ceases, a resynchronization will have to be conducted between the protected server and mirroring server before beginning the replication.

o. If the contingency planning coordinator is considering implementing replication between two sites, the supporting infrastructure for the protected and replicating server also should be considered. Redundant communications paths should be provided if adequate resources are available. The contingency planning coordinator must be aware of potential disadvantages of disk replication, including the possibility that a corrupted disk or data could be replicated, which could destroy the replicated copy.

p. The storage virtualization concept is the process of combining multiple physical storage devices into a logical, virtual storage device that can be centrally managed and is presented to the network applications, operating systems, and users as a single storage pool. Benefits of storage virtualization are that storage devices can be added without requiring network downtime, storage volumes from a downed server or a storage device can be reassigned, and the assigned storage for a server can be easily created, deleted, or expanded on to meet the server's requirements. Virtualization technologies can complement network-attached storage (NAS) environments. NAS environments are file oriented and offer a common storage area for multiple servers. NAS environments are beneficial for file-server applications or storage, such as file sharing or Web and mail services. A NAS device, or server, runs from a minimal operating system and is designed to facilitate data movement. Using file-oriented protocols, any application residing on or any client using virtually any operating system can send data to or receive data from a NAS device.

q. Virtualization technology can also complement a storage area network (SAN), which is a high-speed, high-performance network that enables computers with different operating systems to communicate with one storage device. As opposed to a NAS, a SAN provides data access in blocks and is built to handle storage and backup traffic as opposed to file-oriented traffic. A SAN can be local or remote (within a limited distance) and usually communicates with the server over a fiber channel. The SAN solution moves data storage off the LAN, thus enabling backup data to be streamed to high-speed tape drives, which does not affect network resources as distributed and centralized backup architecture does. Virtualization, NAS, and SAN move away from the client/server architecture and toward the data-centric architecture. If the system manager is considering implementing a data-centric architecture, the advantages and disadvantages of the technologies and the system manager's needs of a data-centric network should be considered. The internet small computer system interface (iSCSI) is a transmission control protocol/internet protocol-based storage networking specification that complements NAS and SAN technology. iSCSI transmits native small computer system interfaces over a layer of the Internet Protocol (IP) stack, which facilitates long-distance storage deployment, management, and data transfer over the IP network. iSCSI enables any storage connected to an IP network to be backed up from any point on that network. With iSCSI, storage and servers can be added at any location and not be restricted by distances, as with SAN. Figure 5–3 graphically shows the level of server availability provided by various contingency solutions.

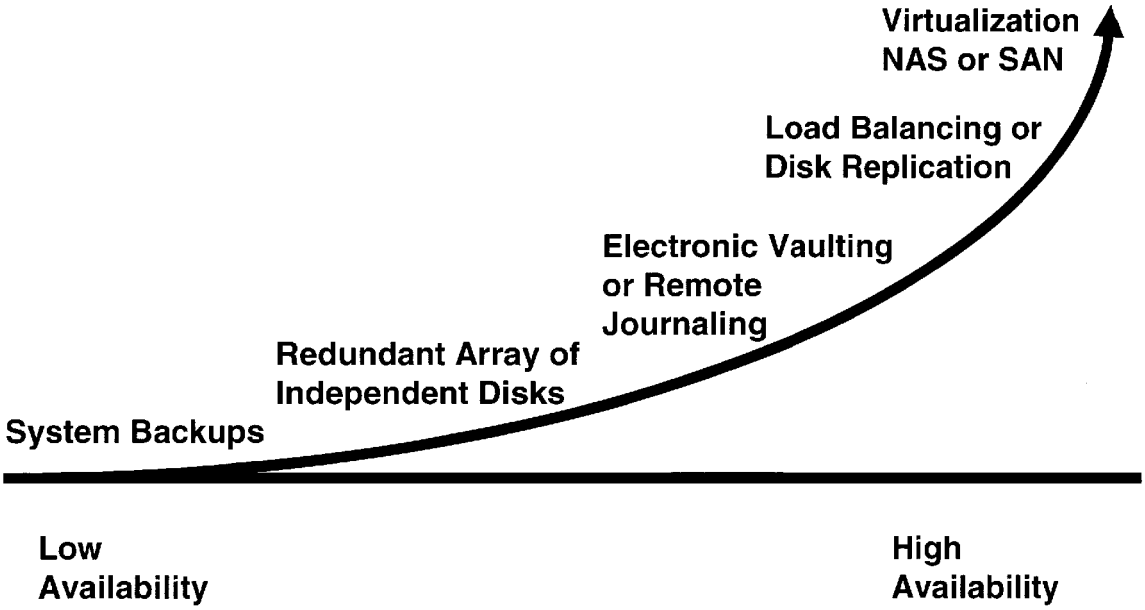


Figure 5–3. Server contingency solutions and availability

5–3. Web sites

Web sites present information to the public or authorized personnel via the World Wide Web or a private intranet. An external Web site also may be an electronic commerce (e-commerce) portal, through which the organization may provide services over the Internet. A Web site may be used internally within an organization to provide information, such as corporate policies, human resources forms, or a phone directory to its employees. Figure 5–4 provides an overview of contingency strategies for Web sites.

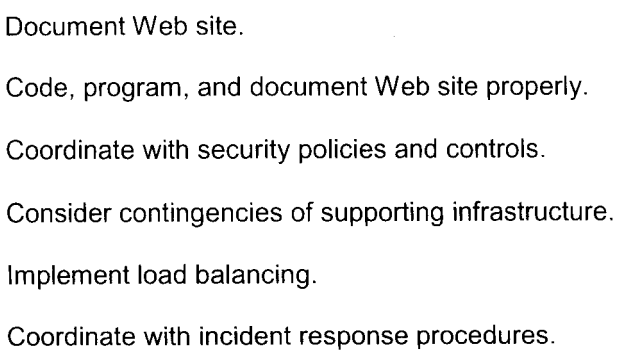


Figure 5–4. Web site contingency strategies

a. In addition to the information presented in paragraph 5–2 of this publication, several factors should be considered when determining the Web site recovery strategy. Practices for Web site contingency planning include the following measures:

(1) Document the Web site. Document the hardware, software, and their configurations used to create and host the Web site.

(2) Program the Web site. As with other applications, Web sites should undergo thorough testing on test servers before production. A configuration management program should be maintained, and changes should be documented appropriately. Approved versions are recorded on CDs for easy storage.

(3) Code the Web site. A Web site is hosted on a server that is assigned an IP address. That IP address maps to a domain name, or Uniform Resource Locator (URL), by a Domain Name Server (DNS). The Web site may not have IP addresses or domain names programmed into the code. If the Web site were recovered at an alternate site, the server could be assigned a different IP address. If the Web site contained hard-coded IP addresses, domain names, or drive letters, the system recovery could be delayed.

(4) Coordinate contingency solutions with appropriate security policies and security controls. A Web site often is the entry point for a hacker into an organization's network. Thus, the Web server and supporting infrastructure should be protected through strong security controls. Contingency planning measures should be coordinated with these controls to ensure that security is not compromised during system recovery. Thus, the appropriate security controls and patches should be implemented on the Web sites that are rebuilt after being compromised.

(5) Coordinate contingency solutions with incident response procedures. Because an external Web site provides an image of the organization to the public, the organization's public image could be damaged if the Web site were defaced or taken down by a cyber attack. To reduce the consequences of such an attack, contingency solutions listed below should be coordinated closely with incident response procedures designed to limit the impacts of a cyber incident.

(6) Use results from the BIA. Impacts and priorities discovered through the BIA of associated major applications and general support systems should be reviewed to determine related requirements.

b. Web site contingency solutions ensure the reliability and availability of the Web site and its resources. Web pages that do not change in content are considered static, whereas Web pages that change in content are called dynamic pages. Dynamic pages are a result of multiple transactions initiated from either or both the client and the server. The content presented in dynamic pages may be stored on a server other than the Web site, such as a protected server behind a firewall. Thus, when choosing contingency solutions for a Web site, the Web site's supporting infrastructure should be considered carefully. In addition to servers, the supporting infrastructure could include the LAN hosting the Web site. Because of the number of requests Web sites could receive and process, load balancing is a popular contingency solution. Load balancing uses the cluster approach, in which Web traffic is balanced across at least two servers. Web clustering is not apparent to the user because it appears as if one server is answering the request.

Therefore, if one server were to fail, traffic would be directed to the operational server. Load balancing can be accomplished through two approaches:

(1) *DNS.* When a user enters an URL using the Web browser, the request is directed to a DNS server that maps the URL to an IP address. The IP address is assigned to the Web server. The DNS server then directs the request to one of the clustered servers. One common DNS approach is the "round robin" method used by the Berkeley Internet Name Daemon.

(2) *Reverse proxy.* The reverse proxy approach bundles the requests of the browsers and reduces bandwidth by performing data caching. The proxy server is logically located between the client and the Web servers, where it receives client requests and forwards them to the Web servers. The server returns the response to the proxy, and the proxy forwards the response to the requesting client. With this method, one IP address is needed. To further segment traffic, the servers can be placed on different subnets to prevent a single subnet from being overloaded. In addition, logs can be collected and monitored in one location, which is the reverse proxy. The administrator also can determine the delegation configuration; therefore, if one machine crashes, the delegation configuration of the reverse proxy can be reconfigured. The result is that the crashed server will not return errors to the requesting browser.

5–4. Army Knowledge Online

a. AKO provides organizations and individuals with the ability to continue to operate through the Web (from outside of the Army network) in the event that their office computers, LAN, or their office itself is not available. These capabilities can be used routinely to work from home, while on the road, during planned contingency exercises, and during ad hoc opportunities such as snow days. Routine use is the best way to exercise the skills needed during a contingency, and best tailors the information which individuals have stored on AKO to support their work. The following functions can be used to continue operations:

(1) Push information to all members of the organization. Groups can be prepared ahead of time and exercised for emergency notification via Web mail/e-mail distribution. Such groups should be maintained and exercised, to include the use of recall rosters with telephone numbers. Web mail provides a redundant means of communication in the event that telecommunications networks are congested or inoperable, which can be more effective in contacting individuals who are traveling and can persist until it is checked, unlike a missed phone call. These information pushes can provide immediate instructions and direct individuals to authoritative sources for status and operating instructions.

(2) Provide a virtual assembly area on the Web. This allows members of an organization to individually pull information from an access controlled Web site designated as the authoritative source for the organization. Contingency pages on AKO should be developed as part of contingency planning, prominently linked from subordinate organization AKO pages and Web sites, and be included as part of contingency training and exercises.

(3) Provide Web access to Army information systems. The AKO portal provides a growing capability to find a wide range of web-based Army information systems, and a method of controlling access to them through the AKO login (Single Sign On).

(4) Provide web storage of information. Organizations and individuals can also use AKO to store work files and references, in a web space they can make available to the Army, their select group, or to themselves. This enables the many different functional specialists in the Army to individually tailor the information available to continue their missions for their organizations in a contingency scenario.

(5) Enable collaboration with individuals and groups. In addition to an Armywide white pages e-mail directory, AKO provides a Web-based capability for chat and instant messaging for more real time communication and collaboration. For more deliberate analysis, forums can be established to maintain a threaded discussion of a topic of interest, and standing forums can be used to find and collaborate with subject matter experts.

b. AKO should be incorporated into the planning, notification/activation, recovery, and reconstitution phases of contingency activities:

(1) *Planning.*

(a) Assign responsibility for establishing and maintaining policy and procedures on the use of AKO during contingencies, AKO groups for notifications, contingency pages, and training within the organization.

(b) Prepare AKO groups and contingency pages on AKO and, as needed, on AKO–S. Establish links from organizational AKO pages and Web sites to assist individuals (for example, new employees not yet trained or family members) in finding the contingency site during an event.

(c) Train individuals on contingency policy and procedures, AKO capabilities, and equip them with common access cards (CAC) and CAC reader devices for their laptops and home computers. Routine use of these capabilities is the best preparation of individuals for a contingency scenario.

(d) The better the preparation, the smoother the transition to Web-based operations. Those organizations and individuals whose mission does not require them to physically touch materiel or people could be operated as a virtual organization over AKO for a theoretically unlimited period. All organizations can use AKO to greatly improve their ability communicate and adapt to a contingency Scenario. Organizations are recommended to systematically encourage the use of these capabilities while traveling, during exercises, as part of a telecommuting program, and routinely from the office desktop.

(2) *Notification/activation.*

(a) Distribute notification messages to groups and post status and instructions to the contingency page.

(b) Distribute quick reference training materials to individuals instructing the use of AKO to conduct business and communicate during a contingency scenario. Their materials may be unavailable, and specific new resources may be added.

(3) *Recovery/reconstitution.* During the recovery and reconstitution phases, Web-based operations on AKO can continue seamlessly as local area network and PC-based capabilities are reestablished. An effective after action review should be conducted to determine what files and information was missing from AKO that would have assisted during the event and ensure the information is posted to AKO.

5–5. Local area networks

a. Lan overview. A LAN is owned by a single organization; it can be as small as two PCs attached to a single hub, or it may support hundreds of users and multiple servers. An overview of contingency strategies for LANs is provided at figure 5–5. An example of a LAN is presented at Figure 5–6. Several topologies are possible when designing a LAN. A protocol is a set of rules used between end points that govern a connection. The protocol determines how the sending and receiving nodes format the data packet. One of the main network standards, Ethernet (both 10/100 and 10 gigabit), may be implemented on a LAN, in addition to less common standards such as Token Ring, asynchronous transfer mode (ATM), fiber distributed data interface. LANs can also be implemented in two main architectures:

(1) *Peer-to-peer*. Each node has equivalent capabilities and responsibilities. For example, five PCs can be networked through a hub to share data.

(2) *Client/server*. Each node on the network is either a client or a server. A client can be a PC or a printer where a client relies on a server for resources.

b. LAN topology. A LAN's topology (several examples of which are described in fig 5–7), protocol, architecture, and nodes will vary depending on the organization. Thus, contingency solutions for each organization will be different.

Document LAN.

Coordinate with vendors.

Coordinate with security policies and controls.

Identify single points of failure.

Implement redundancy in critical system components.

Monitor LAN.

Integrate remote access and wireless local area network technology.

Figure 5–5. LAN contingency strategies

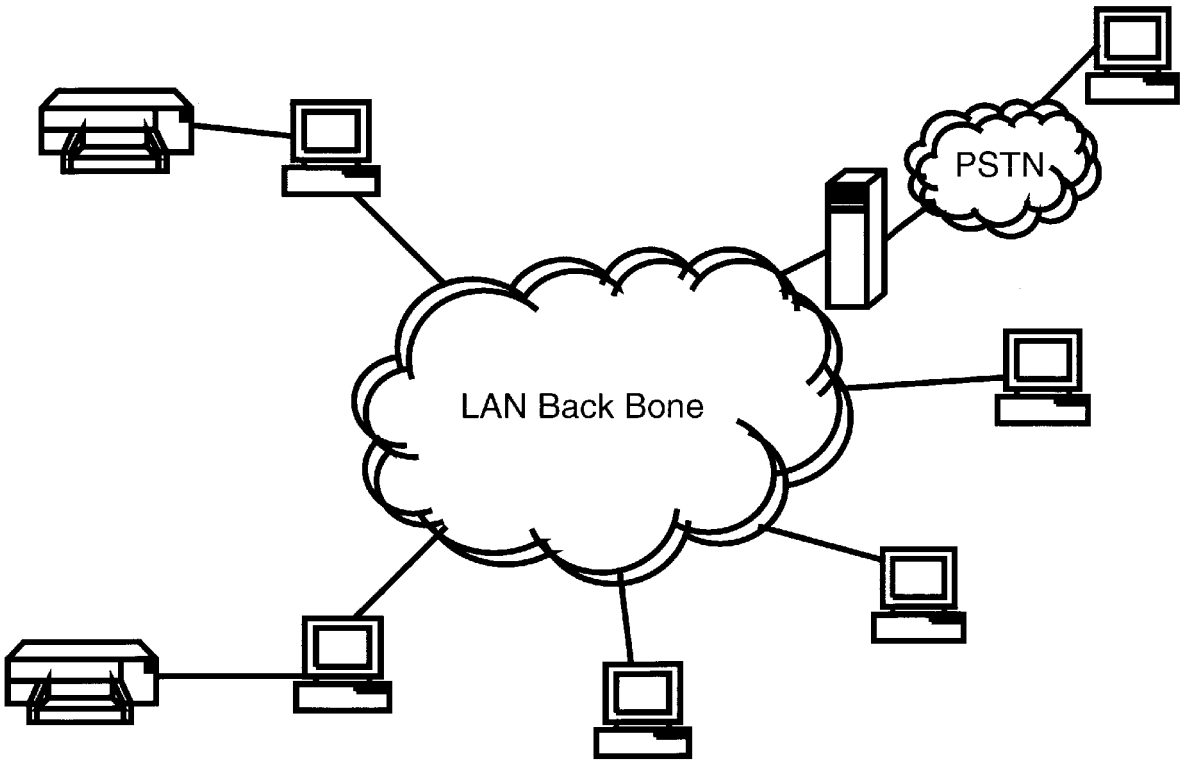


Figure 5–6. Sample LAN

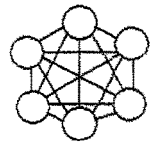
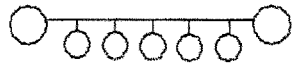
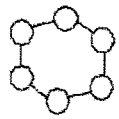
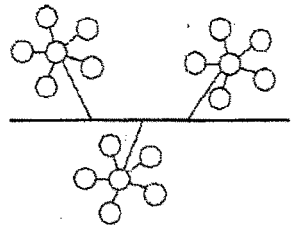
Topology	Diagram
Mesh Networked components are connected with many redundant interconnections between network nodes. In a true mesh topology, every node has a connection to every other node in the network.	
Star All nodes are connected to a central hub.	
Bus All nodes are connected to a central cable, called the bus or backbone.	
Ring All nodes are connected to one another in the shape of a closed loop so that each node is connected directly to two other nodes, one on either side of it.	
Tree A tree is a hybrid topology where a linear bus backbone connects star-configured networks.	

Figure 5–7. LAN topologies

c. Contingency considerations. When developing the LAN recovery strategy, the contingency planning coordinator should follow the information presented earlier regarding desktops, servers, and Web sites. In addition, the following practices should be considered:

(1) *LAN documentation.* The physical and logical LAN diagram should be up to date. The physical diagram should display the physical layout of the facility that houses the LAN, and cable jack numbers should be documented on the physical diagram. The logical diagram should present the LAN and its nodes. Network discovery software can provide an accurate picture of the LAN. Both diagrams help recovery personnel to restore LAN services more quickly.

(2) *System configuration and vendor information documentation.* Document configurations of network connective devices that facilitate LAN communication (for example, switches, bridges, and hubs) to ease recovery. Vendors and their contact information should be documented in the contingency plan to provide for prompt hardware and software resupply.

(3) *Coordination with security policies and security controls.* LAN contingency solution(s) should be coordinated with network security policies to protect against threats that could disrupt the network. Therefore, in choosing the appropriate technical LAN contingency solution(s), similar security controls and security-related activities (for example, risk assessment, vulnerability scanning) in the production systems should be implemented in the contingency

solution(s) to ensure that, during a network disruption, executing the technical contingency solution(s) does not compromise or disclose sensitive data.

(4) *Use of results from the BIA.* Impacts and priorities discovered through the BIA of associated major applications and general support systems should be reviewed to determine LAN recovery priorities.

d. Contingency solutions. When developing the LAN contingency plan, the contingency planning coordinator should identify single points of failure that affect critical systems or processes outlined in the BIA. This analysis could include threats to the cabling system, such as cable cuts, electromagnetic and radio frequency interference, and damage resulting from fire, water, and other hazards. Standard Army IT designs call for flood wiring to accommodate adds, moves, and changes. Current Army standards calls for fiber backbone cable (using high-speed fiber optic cabling) that provides spare capacity.

(1) Often, it is not cost effective to run duplicate cables to each computer jack. However, each desktop jack usually is equipped with at least one phone jack and computer jack. When cables are installed, an organization may choose to install an extra data or phone jack every few drops; then, if a problem does occur in a cable run, an extra jack within a short distance would be available as backup. In this case, temporary cable can be run from the desktop to the extra jack to provide connectivity for the desktop until a new cable can be run to the problem jack. Also, if the phone system's connectivity block is located in the same location as the backbone hubs, a phone jack can be converted easily into a data jack, if the phone jack provides the appropriate bandwidth.

(2) Contingency planning also should consider network connecting devices, such as hubs, switches, routers, and bridges. The BIA should characterize the roles that each device serves in the network, and a contingency solution should be developed for each device based on its BIA criticality. As an example of a contingency strategy for network connecting devices, redundant intelligent network routers may be installed in a network, enabling a router to assume the full traffic workload if the other router failed. A more cost-effective approach would be to include structured cabling systems according to Army standards that allow for spare capacity and flexibility in the horizontal cabling. Also, planners should take into consideration the need for power supply redundancies for voice-over IP systems.

(3) Remote access is a service provided by servers and devices on the LAN. Remote access provides a convenience for users working offsite or allows for a means for servers and devices to communicate between sites. Remote access can be conducted through various methods, including dialup access and virtual private network (VPN). If an emergency or serious system disruption occurs, remote access may serve as an important contingency capability by providing access to organizationwide data for recovery teams or users from another location. If remote access is established as a contingency strategy, data bandwidth requirements should be identified and used to scale the remote access solution. Additionally, security controls such as one-time passwords and data encryption should be implemented if the communications contains sensitive information.

(4) Wireless LANs and multiple area networks can serve as an effective contingency solution to restore network services following a wired LAN disruption. Wireless networks do not require the cabling infrastructure of conventional LANs; therefore, they may be installed quickly as an interim or permanent solution. However, wireless networks broadcast the data over a radio signal, enabling the data to be intercepted. When implementing a wireless network, security controls, such as data encryption, must be implemented in accordance with AR 25–2 if the communications traffic contains sensitive information.

(5) To reduce the effects of a LAN disruption through prompt detection, monitoring software can be installed. The monitoring software issues an alert if a node begins to fail or is not responding. The monitoring software can facilitate troubleshooting and often provides the administrator with a warning before users and other nodes notice problems. Many types of monitoring software may be configured to send an electronic page to a designated individual automatically when a system parameter falls out of its specification

5–6. Wide-area networks

a. WAN overview. In addition to connecting LANs, a WAN also can connect to another WAN, or it can connect a LAN to the Internet. A sample WAN diagram is found in figure 5–8 and an overview of WAN contingency strategies is provided in figure 5–9. Types of WAN communication links include the following methods:

(1) Dialup. Dialup connections over modems can provide minimal data transfer over a nonpermanent connection. The speed will depend on the modems used, up to 56 kilobits per second (kbps).

(2) Integrated services digital network (ISDN). ISDN is an international communications standard for sending voice, video, and data over digital or standard telephone wires. ISDN supports data transfer rates of 64 or 128 kbps.

(3) T–1. T–1 is a dedicated phone connection supporting data rates of 1.544 megabits per second (Mbps). A T–1 line consists of 24 individual 64-kbps channels, and each channel can be configured to carry voice or data signals. Fractional T–1 access also can be provided when multiples of 64-kbps lines are required.

(4) T–3. T–3 is a dedicated phone connection supporting data rates of about 43 Mbps. A T–3 line consists of 672 individual channels, each of which supports 64 kbps.

(5) Frame relay. Frame relay is a packet-switching protocol for connecting devices on a WAN. In frame relay, data is routed over virtual circuits. Frame relay networks support data transfer rates at T–1 and T–3 speeds.

(6) ATM. ATM is a network technology that transfers data at high speeds using packets of fixed size. Implementations of ATM support data transfer rates of from 25 to 622 Mbps and provides guaranteed throughput.

(7) Synchronous optical network (SONET). SONET is the standard for synchronous data transmission on optical media and supports gigabit transmission rates.

(8) Wireless. A wireless LAN bridge can connect multiple LANs to form a WAN. Wireless supports distances of 20 to 30 miles with a direct line of sight.

(9) VPN. A VPN is an encrypted channel between nodes on the Internet. While a VPN is not a WAN, it is a technology that uses WANs to provide a virtual network for users in various locations.

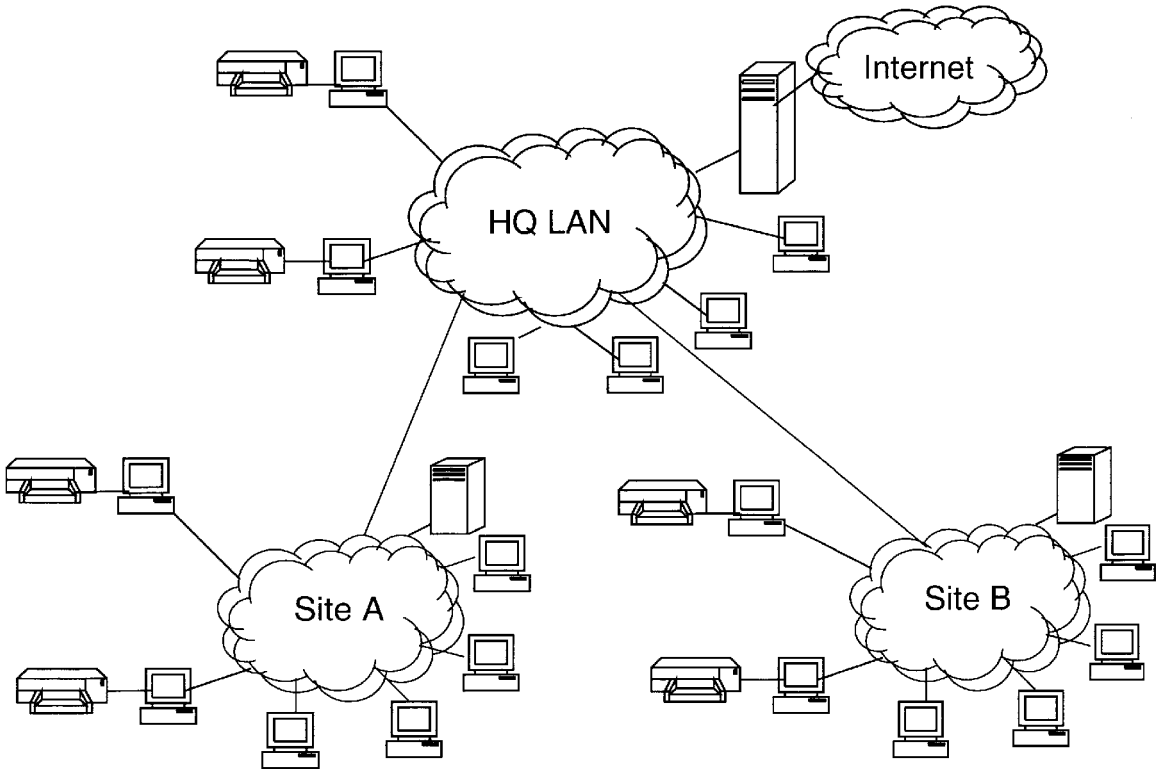


Figure 5–8. Wide-area networks

Document WAN.

Coordinate with vendors.

Coordinate with security policies and controls.

Identify single points of failure.

Implement redundancy in critical system components.

Institute SLAs.

Figure 5–9. WAN contingency strategies

b. Contingency considerations. WAN contingency considerations should enhance the ability of recovery personnel to restore WAN services after a disruption. The practices listed below complement WAN recovery strategies to create a more comprehensive WAN contingency capability:

(1) Document WAN. The WAN architecture diagram should be kept up to date and should identify network connecting devices, unit addresses (IP addresses), and types of communication links and vendors.

(2) Document systems configurations and vendors. Document configurations of media access unit devices that facilitate WAN communication to ease recovery. The contingency plan should include a vendor list to enable rapid replacement of hardware, software, and other WAN components following a disruption. The plan also should document the communications providers, including POC and contract information.

(3) Coordinate with security policies and security controls. WAN contingency solution(s) should be coordinated with network security policies to protect against threats that could compromise network availability. Thus, in choosing the appropriate technical contingency solution(s), similar security controls and security-related activities (for example, risk assessment, vulnerability scanning) in the production environment should be implemented in the contingency solution(s) to ensure that, during a disruption to WAN connectivity, executing the technical contingency solution(s) does not compromise or disclose sensitive data.

(4) Use results from the BIA. Impacts and priorities discovered through the BIA of associated major applications and general support systems should be reviewed to determine related requirements.

c. Contingency solutions. WAN contingency solutions include all of the measures discussed for PCs, servers, Web sites, and LANs. In addition, WAN contingency planning should consider the communications links that connect the disparate LANs. WAN contingency strategies are influenced by the type of data routed on the network. A WAN that hosts a mission-critical distributed system may require a more robust recovery strategy than a WAN that connects multiple LANs for simple resource sharing purposes. Organizations should consider the following contingency solutions for ensuring WAN availability:

(1) Redundant communications links. Redundant communications links usually are necessary when the network processes critical data. The redundant links could be the same type, such as two T–1 connections, or the backup link could provide reduced bandwidth to accommodate only critical transmissions in a contingency situation. For example, an ISDN line could be used as a contingency communications link for a primary T–1 connection. If redundant links are used, the Contingency Planning Coordinator should ensure that the links have physical separation and do not follow the same path; otherwise, a single incident, such as a cable cut, could disrupt both links.

(2) Redundant network service providers. If 100-percent data availability is required, redundant communications links can be provided through multiple Network Service Providers (NSPs). If this solution is chosen, the manager should ensure that the NSPs do not share common facilities at any point, including building entries or demarcations.

(3) Redundant network connecting devices. Duplicate network connecting devices, such as routers, switches, and firewalls, can create high availability at the LAN interfaces and provide redundancy if one device fails. Duplicate devices also provide load balancing in routing traffic.

(4) Redundancy from network service provider (NSP) or Internet service provider. The Contingency Planning Coordinator should consult with the selected NSP or ISP to assess the robustness and reliability within their core networks (for example, redundant network connecting devices and power protection). The contingency planning coordinator should also be aware of NIPRNet connectivity to supported camps, posts, and stations.

(5) To provide further redundancy, independent Internet connections may be established from two geographically separated LANs. If one connection were to fail, Internet traffic could be routed through the remaining connection. However, this strategy highlights the balance that should be maintained between security and availability. Multiple Internet connections increase a network's vulnerability to hackers. Therefore, as emphasized previously, contingency strategies should be weighed against security considerations at all times.

(6) SLAs can facilitate prompt recovery following software or hardware problems associated with the network. A SLA also may be developed with the NSP or ISP to guarantee the desired network availability and establish tariffs if the vendor's network is unavailable. If the NSP or ISP is contracted to provide network-connecting devices, such as routers, the availability of these devices should be included in the SLA.

5–7. Distributed systems

Distributed systems are implemented in environments in which clients and users are widely dispersed. These systems rely on LAN and WAN resources to facilitate user access and the elements comprising the distributed system require synchronization and coordination to prevent disruptions and processing errors. A common form of distributed systems is a large database management system that supports agency-wide business functions in multiple geographic locations. In this type of application, data are replicated among servers at each location, and users access the system from their local server. An overview of contingency strategies for distributed systems is provided in figure 5–10.

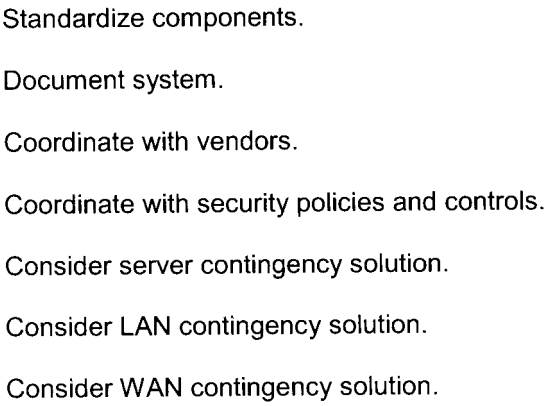


Figure 5–10. Distributed system contingency strategies

a. Overview of distributed systems. A distributed system is an interconnected set of multiple autonomous processing elements, configured to exchange and process data to complete a single business function. To the user, a distributed system appears to be a single source. Distributed systems use the client-server relationship model to make the application more accessible to users in different locations.

b. Contingency considerations. Contingency considerations for the distributed system draw on the concepts discussed for the previous platforms. Because the distributed system relies extensively on local and wide area network connectivity, distributed system contingency measures are similar to those discussed for LANs and WANs.

(1) Standardize hardware, software, and peripherals. System recovery may be expedited if hardware, software, and peripherals are standardized throughout the distributed system. Recovery costs may be reduced because standard configurations may be designated and resources may be shared. Standardized components also reduce system maintenance across the organization.

(2) Document systems configurations and vendors. Document the distributed system's architecture and the configurations of its various components. In addition, the contingency plan should identify vendors and model specifications to facilitate rapid equipment replacement after a disruption.

(3) Coordinate with security policies and security controls. Distributed system contingency solution(s) should be coordinated with network security policies where similar security controls and security-related activities (for example, risk assessment, vulnerability scanning) in the production environment should be implemented in the contingency solution(s) to ensure that, during a system disruption, executing the technical contingency solution(s) does not compromise or disclose sensitive data.

(4) Use results from the BIA. Impacts and priorities discovered through the BIA of associated LAN and/or WAN should be reviewed to determine recovery requirements and priorities.

c. Contingency solutions. Because a distributed system spans multiple locations, risks to the system and its supporting infrastructure should be analyzed thoroughly in the BIA process. As discussed above, distributed system contingency strategies typically reflect the system's reliance on LAN and WAN availability. Contingency solutions may be built into the distributed system during design and implementation. A distributed system, for example, may be constructed so that all data resides in one location (such as the organization's headquarters) and is replicated to the local sites. Changes at local sites could be replicated back to headquarters. If data are replicated to the local sites as read only, the data in the distributed system are backed up at each local site. This means that if the headquarters server were to fail, data could still be accessed at the local sites over the WAN. Conversely, if data were uploaded hourly from local sites to the headquarters' site, then the headquarters' server would act as a backup for the local servers. As the example above illustrates, the distributed system typically provides some inherent level of redundancy that can be incorporated in the contingency strategy. For example, consider a critical system that is distributed between an agency headquarters and a small office. Assuming data are replicated at both sites, a cost-effective recovery strategy may be to establish a reciprocal agreement between the two sites. Under this agreement, in the event of a disruption at one office, essential personnel would relocate to the other office to continue to process system functions. This strategy could save significant contingency costs by avoiding the need to procure and equip alternate sites. On the basis of strategy, when developing a distributed system contingency strategy, the following technologies should be considered because they were addressed for LANs and WANs:

(1) System backups.

(2) RAID.
(3) Redundancy of critical system components.
(4) Electronic vaulting and remote journaling.
(5) Disk replication.
(6) Virtualization, NAS, or SAN.
(7) Remote access.
(8) Wireless networks.
(9) LAN cabling system redundancy.
(10) WAN communication link redundancy.

5–8. Mainframe systems

Unlike the client/server architecture, the mainframe architecture is centralized. The clients that access the mainframe are "dumb" terminals with no processing capabilities. The dumb terminals accept output only from the mainframe. However, PCs also can access a mainframe by using terminal emulation software. An overview of contingency strategies for mainframe systems in provided in figure 5–11.

Back up data and store offsite.

Document system.

Coordinate with vendors.

Coordinate with security policies and controls.

Implement redundancy and fault tolerance in critical system components.

Consider hot site or reciprocal agreement.

Institute vendor SLAs.

Replicate data.

Implement storage solutions.

Use uninterruptible power supplies.

Figure 5–11. Mainframe contingency strategies

a. Overview of mainframe systems. A mainframe is a multiuser computer designed to meet the computing needs of a large organization. The term was created to describe the large central computers developed in the late 1950s and 1960s to process bulk accounting and information management functions. Mainframe systems store all data in a central location rather than dispersing data among multiple machines, as with distributed systems.

b. Contingency considerations. Although the mainframe computer is large and more powerful than the platforms discussed previously, it shares many of the same contingency requirements. Because a mainframe uses a centralized architecture, the mainframe does not have the inherent redundancy that a distributed system or network provides. As a result, mainframe availability and data backups are critical. The following measures should be considered when determining mainframe contingency requirements:

(1) Store backup media offsite. Backup media should be labeled, logged, and stored offsite in a secure, environmentally controlled facility. The storage facility should be located far enough away from the original site to reduce the likelihood that both sites would be affected by the same event.

(2) Document system configurations and vendors. Maintaining detailed records of system configurations enhances system recovery capabilities. In addition, vendors that supply essential hardware, software, and other components should be identified in the contingency plan.

(3) Coordinate with network security policy and system security controls. Mainframe contingency solutions should be coordinated with network security policies, such as stringent access controls. Network security controls can help protect against attacks that could compromise the mainframe's availability.

(4) Utilize results from the BIA. Impacts and priorities discovered through the BIA of associated major applications and general support systems should be reviewed to determine recovery requirements and priorities.

c. Contingency solutions. Mainframes require different contingency strategies from distributed systems because data is stored in a single location. Contingency strategies should emphasize the mainframe's data storage capabilities and underlying architecture. Redundant system components are critical to ensure that a failure of a system component, such as a power supply, does not cause a system failure. UPS and power monitoring and management systems also should be used to ensure power fluctuation will not affect the mainframe. Because mainframes typically process large, critical applications, a long-term backup power solution may be needed. A gas or diesel generator can ensure that mainframe processing is not interrupted by a power outage.

(1) Disk redundancy can be provided for the DASDs by implementing a RAID solution.

(2) A contingency strategy is to have a replacement system available at an alternate warm or hot site because each mainframe architecture is unique and centralized. However, backup mainframe platforms are very costly to purchase and maintain so many agencies share commercial systems. Agencies also typically maintain vendor support contracts to repair the damaged unit. However, vendor support alone may not restore system functions within the allowable outage time. In all cases, vendor SLAs should be kept up to date and reviewed to ensure that the vendor provides adequate support to meet system availability requirements.

(3) Mainframes should be backed up regularly and backup media should be stored offsite. Backup and retention schedules should be based on the criticality of the data being processed and the frequency that the data are modified. As with servers, remote journaling or electronic vaulting to the alternate site could be an effective technical contingency solution. In addition, disk replication, virtualization, or NAS or SAN technologies that replicate various platforms to one replicating server could be used in some cases.

(4) A variety of actions should be undertaken to prepare for and recover from contingency situations. A summary is provided in table 5–1. The boxes marked with an X suggest what actions might be prudent for the system attributed to the column.

Table 5–1
Contingency strategy summary

Contingency consideration	Desktop computer/ portable system	Server	Web site	Local area network	Wide area network	Distributed system	Mainframe system
Contingency considerations							
Document system, configurations, and vendor information	X	X	X	X	X	X	X
Encourage individuals to back up data	X						
Code, program, and document properly			X				
Coordinate contingency solution with security policy	X	X	X	X	X	X	X
Coordinate contingency solution with system security controls	X	X	X	X	X	X	X
Consider contingencies of supporting infrastructure			X			X	
Consider hot site and reciprocal agreements							X
Coordinate with incident response procedures			X				
Coordinate with vendors				X	X	X	X
Institute vendor SLAs					X		X

Table 5–1
Contingency strategy summary—Continued

Contingency consideration	Desktop computer/ portable system	Server	Web site	Local area network	Wide area network	Distributed system	Mainframe system
Provide guidance on saving data on personal computers	X						
Standardize hardware, software, and peripherals	X	X				X	
Store backup media offsite	X	X					X
Store software offsite	X	X					
Contingency solutions							
Back up system, applications, and/or data	X	X					
Ensure interoperability among components	X	X					
Identify single points of failure				X	X		
Image disks	X						
implement fault tolerance in critical components		X					X
Implement load balancing		X	X				
Implement redundancy in critical components	X	X		X	X		X
Implement storage solutions		X					X
Integrate remote access and wireless technologies				X			
Monitor				X			
Replicate data		X					X
Use alternate hard drives	X						
Use uninterruptible power supplies	X	X					X

Chapter 6
IT Contingency Plan Services

6–1. Contingency support for information services

The installation commander:

a. Requires the installation staff and tenant activities to develop information systems requirements in their contingency plans.

b. Provides contingency information service requirements to the DOIM.

c. Advises the DOIM of emergency situations that might involve the installation.

d. Develops policy and procedures appropriate to the installation mission and locations for lighting, blackout, and other emergency conditions.

6–2. Emergency information technology services

a. Establishing stand-alone emergency action console (EAC) telephone switching systems and electronic switching system remote consoles, with attendant operator requirements within Army command operation centers, has been overtaken by technology. Information exchange service, for which United States Army Information Systems Engineering Command is responsible, is provided by automated display telephone sets operated by command operation center action officers.

b. Electronic switches are designed to provide for automatic circuit transfer of selected command and control circuits, DSN circuits, off-hook circuits, and confirmation circuits to command operation center controls, in the event of a catastrophic failure of the administrative telephone system.

c. When mission requirements justify, command and control functions and emergency integrated voice and data services are provided by the switch serving the installation. Multiple and separate ingress/egress routes are provided for switches engineered with command and control and emergency voice service. Europe and other overseas areas are not included in this policy and may continue operating stand-alone EACs.

6–3. Mobilization information services support planning

a. Mobilization information services support planning should consider the impact of the surge in the use of information services. During the operational readiness improvement phase, information services need to be extended to support Reserve Component forces while at the mobilization station (MS). Mobilization essential information services expected to be operational during all phases of mobilization include the following categories:

(1) Administrative telephone service.

(2) Data processing. This includes information processing facilities, Army Standard Information System access, and other data processing capabilities.

(3) Facsimile.

(4) High frequency radio.

(5) Nontactical radio.

(6) Secure voice.

(7) Record communications.

(8) Global command and control system access.

(9) Print plant facilities.

(10) Records management facilities.

b. During the premobilization (peacetime) period, mobilization requirements for additional leased telephone service and long-haul communications circuits should be defined. Mobilization DA Form 3938 (Local Service Request and Request for Service) documentation is developed and retained by the DOIM for implementation at mobilization.

c. Designated DOIM offices have a supporting installation responsibility to provide mobilization information services planning assistance to designated semiactive and State-operated MS.

6–4. Alternate sites

a. Although major disruptions with long-term effects may be rare, they should be accounted for in the contingency plan. Thus, the plan should include a strategy to recover and perform system operations at an alternate facility for an extended period. In general, three types of alternate sites are available:

(1) Dedicated site owned or operated by the organization.

(2) Reciprocal agreement or memorandum of agreement with an internal or external entity.

(3) Commercially leased facility.

b. Regardless of the type of alternate site chosen, the facility should be able to support system operations as defined in the contingency plan. The three alternate site types may be categorized in terms of their operational readiness. Based on this factor, sites may be identified as cold sites, warm sites, hot sites, mobile sites, and mirrored sites. Progressing from basic to advanced, the sites are described below and summarized in table 6–1.

Table 6–1
Alternate site criteria selection

Site	Cost	Hardware equipment	Telecommunications	Setup time	Location
Cold Site	Low	None	None	Long	Fixed
Warm site	Medium	Partial	Partial/full	Medium	Fixed
Hot site	Medium/high	Full	Full	Short	Fixed
Mobile site	High	Dependent	Dependent	Dependent	Not fixed
Mirrored site	High	Full	Full	None	Fixed

(1) Cold sites typically consist of a facility with adequate space and infrastructure (electric power, telecommunications connections, and environmental controls) to support the IT system. The space may have raised floors and other attributes suited for IT operations. The site does not contain IT equipment and usually does not contain office automation equipment, such as telephones, facsimile machines, or copiers. The organization using the cold site is responsible for providing and installing necessary equipment and telecommunications capabilities. Cold sites and the

resources to use them, however, are usually not immediately available and the site may be hard to reserve for operational testing.

(2) Warm sites are partially equipped office spaces that contain some or all of the system hardware, software, telecommunications, and power sources. The warm site is maintained in an operational status ready to receive the relocated system. The site may need to be prepared before receiving the system and recovery personnel. In many cases, a warm site may serve as an operational facility for another system or function, and in the event of contingency plan activation, the usual activities are displaced temporarily to accommodate the disrupted system. As with cold sites, but to a lesser extent, warm sites and the resources to use them are usually not immediately available and the site may be hard to reserve for operational testing.

(3) Hot sites are office spaces appropriately sized to support system requirements and configured with the necessary system hardware, supporting infrastructure, and support personnel. Hot sites are typically staffed 24 hours a day, 7 days a week. Hot site personnel begin to prepare for the system arrival as soon as they are notified that the contingency plan has been activated. These sites are, however, usually expensive.

(4) Mobile sites are self-contained, transportable shells custom-fitted with specific telecommunications and IT equipment necessary to meet system requirements. These are available for lease through commercial vendors. The facility often is contained in a tractor-trailer and may be driven to and set up at the desired alternate location. In most cases, to be a viable recovery solution, mobile sites should be designed in advance with the vendor, and an SLA should be signed between the two parties. This is necessary because the time required to configure the mobile site can be extensive, and without prior coordination, the time to deliver the mobile site may exceed the system's allowable outage time.

(5) Mirrored sites are fully redundant facilities with full, real-time information mirroring. Mirrored sites are identical to the primary site in all technical respects. These sites provide the highest degree of availability because the data is processed and stored at the primary and alternate site simultaneously. These sites typically are designed, built, operated, and maintained by the organization.

c. There are obvious cost and ready-time differences among the five options. The mirrored site is the most expensive choice, but it ensures virtually 100-percent availability. Cold sites are the least expensive to maintain, however, it may require substantial time to acquire and install necessary equipment. Partially equipped sites, such as warm sites, fall in the middle of the spectrum. In many cases, mobile sites may be delivered to the desired location within 24 hours. However, the time necessary for installation can increase this response time. The selection of fixed-site locations should account for the time and mode of transportation necessary to move personnel there. In addition, the fixed site should be in a geographic area that is unlikely to be negatively affected by the same disaster event (for example, weather-related impacts or power grid failure) as the organization's primary site. Sites should be analyzed further by the organization based on the specific requirements defined in the BIA. As sites are evaluated, the DOIM should ensure that the system's security, management, operational, and technical controls are compatible with the prospective site. Such controls may include firewalls and physical access controls, data remanence controls, and security clearance level of the site and staff supporting the site.

d. These alternate sites may be owned and operated by the organization (internal recovery), or commercial sites may be available under contract. If contracting for the site with a commercial vendor, adequate testing time, workspace, security requirements, hardware requirements, telecommunications requirements, support services, and recovery days (how long the organization can occupy the space during the recovery period) should be negotiated and clearly stated in the contract. Customers should be aware that multiple organizations may contract with a vendor for the same alternate site; as a result, the site may be unable to accommodate all of the customers if a disaster affects enough of those customers simultaneously. The vendor's policy on how this situation should be addressed and how priority status is determined should be negotiated.

e. Two or more organizations with similar or identical IT configurations and backup technologies may enter a formal agreement to serve as alternate sites for each other or enter into a joint contract for an alternate site. This type of site is set up via a reciprocal agreement or memorandum of understanding (MOU). A reciprocal agreement should be entered into carefully because each site should be able to support the other, in addition to its own workload, in the event of a disaster. This type of agreement requires the recovery sequence for the applications from both organizations to be prioritized from a joint perspective, favorable to both parties. Testing should be conducted at the partnering sites to evaluate the extra processing thresholds, compatible system and backup configurations, sufficient telecommunications connections, compatible security measures, and the sensitivity of data that might be accessible by other privileged users, in addition to functionality of the recovery strategy.

f. An MOU, memorandum of agreement (MOA), or an SLA for an alternate site should be developed specific to the organization's needs and the partner organization's capabilities. The legal department of each party should review and approve the agreement. The agreement should always comply with AR 70–1 and address at a minimum, each of the following elements:

(1) Contract/agreement duration.

(2) Cost/fee structure for disaster declaration and occupancy (daily usage), administration, maintenance, testing,

annual cost/fee increases, transportation support cost (receipt and return of offsite data/supplies, as applicable), cost/expense allocation (as applicable), and billing and payment schedules.

(3) Disaster declaration (that is, circumstances constituting a disaster, notification procedures).

(4) Site/facility priority access and/or use.

(5) Site availability.

(6) Site guarantee.

(7) Other clients subscribing to same resources and site, and the total number of site subscribers, as applicable.

(8) Contract/agreement change or modification process.

(9) Contract/agreement termination conditions.

(10) Process to negotiate extension of service.

(11) Guarantee of compatibility.

(12) IT system requirements (including data and telecommunication requirements) for hardware, software, and any special system needs (hardware and software).

(13) Change management and notification requirements, including hardware, software, and infrastructure.

(14) Security requirements, including special security needs.

(15) Staff support provided/not provided.

(16) Facility services provided/not provided (use of onsite office equipment, cafeteria, and so on).

(17) Testing, including scheduling, availability, test time duration, and additional testing, if required.

(18) Records management (onsite and offsite storage, maintenance, and access/release), including electronic media and hardcopy.

(19) Service level management (performance measures and management of quality of IT services provided).

(20) Workspace requirements (for example, chairs, desks, telephone, PCs).

(21) Supplies provided/not provided (for example, office supplies).

(22) Additional costs not covered elsewhere.

(23) Other contractual issues, as applicable.

(24) Other technical requirements, as applicable.

g. All agencies should designate alternate operating facilities as part of their IT contingency plans and prepare their personnel for the possibility of unannounced relocation of MEFs and/or IT contingency staffs to these facilities. Facilities may be identified from existing organization local or field infrastructures, or external sources.

h. Facilities should be capable of supporting operations in a threat-free environment, as determined by the geographical location of the facility, a favorable assessment of the local threat, and/or the collective protection characteristics of the facility. In acquiring and equipping such facilities, agencies are encouraged to consider cooperative interorganization agreements and promote sharing of identified alternate facilities.

i. Alternate facilities should provide—

(1) Intermediate capability to perform MEFs under various threat conditions, including threats involving weapons of mass destruction.

(2) Sufficient space and equipment to sustain the relocating organization. Since the need to relocate may occur without warning or access to operating facilities may be denied, agencies are encouraged to preposition and maintain minimum essential equipment for continued operations at the alternate operating facilities.

(3) Interoperable communications with all identified essential internal and external organizations, critical customers, and the public.

(4) Reliable logistical support, services, and infrastructure systems, including water, electrical power, heating, and air conditioning.

(5) Ability to sustain operations for a period of up to 30 days.

(6) Consideration for the health, safety, and emotional welfare of relocated employees.

(7) Appropriate physical security and access controls.

j. Alternate site and emergency communications.

(1) The success of organizational operations at an alternate facility is absolutely dependent on the availability and redundancy of critical communications systems to support connectivity to internal organizations, other agencies, critical customers, and the public. When identifying communications requirements, agencies should take maximum advantage of the entire spectrum of communications media likely to be available in any emergency situation. These services may include, but are not limited to: secure and/or nonsecure voice, fax, and data, connectivity; Internet access; and e-mail. Interoperable communications should provide—

(a) Capability commensurate with an organization's MEFs and activities.

(b) Ability to communicate with IT contingency staffs, management, and other organizational components.

(c) Ability to communicate with other agencies and emergency personnel.

(d) Access to other data and systems necessary to conduct essential activities and functions.

(2) It is essential that emergency communications planning prepares for the loss of e-mail capability. In the event

that a WAN or LAN is lost, so is any e-mail capability. Other methods such as cellular/wireless (including secure voice phones that are allowed communicate up to top secret), Iridium, and International Maritime Satellite/Enhanced Mobile Satellite Service. It is recommended that at least some of the personnel responsible for carrying out the contingency plan have access to cellular phones and wireless devices that have had Wireless Priority Service (WPS) added to them. Similarly, those personnel should have access to the Government Emergency Telephone Service (GETS). In previous contingency scenarios, landline service was nonexistent and cellular/wireless networks soon became congested. WPS and GETS assists essential and first-responder personnel in getting calls through.

(3) The protection and ready availability of electronic and hardcopy emergency operating records, documents, references, records, and information systems needed to support MEFs at an alternate site under the full spectrum of emergencies is a critical element of a successful IT contingency plan. Organization personnel should have access to and be able to use these records and systems in conducting their essential functions.

6–5. Telework

a. The Army should have plans in place that allow government business to continue during emergency situations. Telework is a virtual resource solution and provides access to resources that may not be available otherwise. Agencies have the flexibility to use teleworkers in emergency situations, but it will not happen spontaneously. A viable ongoing telework program is the foundation that should be in place.

b. Telework provides flexibility in the locations where employees may perform their jobs. Telework lets employees work at home, at an alternate office closer to home, or at other defined locations. Telework may be performed on a fixed schedule or at random. For the Army, perhaps the most important aspect of telework is that it can greatly facilitate COOP in times of crisis. See AR 25–1, paragraph 6–10, and DA Pam 25–1–1, paragraph 7–6, for additional telework policy and procedures.

c. Designated contingency facilities may not have all the staff needed to support MEFs and may not be able to accommodate enough key staff to facilitate maximum government operations. Organizations should make sure that key members of the staff are designated to report to alternate sites, including their home if they telework.

d. Telework is particularly appropriate in times of a pandemic health crisis in which direct contact is discouraged. Although this is not an IT crisis on the surface, losing access to the workforce that supports command, control, communications, and computers (C4)/IT would be. Organizations need find ways to encourage their staff to telework so that MEFs are still being carried out while their staff is more protected from becoming ill or passing illness on to others.

e. To facilitate the use of telework during emergencies, certain steps are necessary. Organizations should—

(1) Have telework agreements in place with teleworkers so that they are already completed when and if the need arises.

(2) Develop a cadre of regularly scheduled “core” teleworkers

(3) Permit teleworkers to experience working offsite and learn to communicate electronically with colleagues and clients by doing it regularly.

(4) Permit supervisors and managers to experience managing employees without face to face contact.

(5) Ensure that teleworkers are aware of and follow the data at rest requirements outlined in AR 25–2, paragraph 4–5.

Chapter 7
IT System Priority

7–1. Prioritization of services

a. During stressed situations, the reduction or denial of information services to some users may be necessary to support essential mission requirements. The stressed situation may be due to a mobilization effort, wartime operation, terrorist activity, civil disturbance, or natural disaster and may result from increased system use or service degradation due to equipment, software, or transmission failure. The direct impact will be that provisions of quality information service will not be possible. User access to some systems should be restricted or denied to ensure essential operational users are supported.

b. Guidelines are provided by the National Communications System (NCS) for reduction of information transfer traffic in an emergency (see the MINIMIZE policy in AR 25–10) and communications circuit restoration priority system procedures. However, these do not apply to most installation information service users for COOP, telephone service, or data processing support.

7–2. Prioritization scheme

a. The following prioritization scheme criteria are used for the prioritization of information services provided users not assigned an NCS priority:

(1) Priority 1: System use associated with essential command and control operations.

(2) Priority 2: Systems use associated with essential security, safety, and fire operations.

(3) Priority 3: Systems use essential for national emergency, mobilization, or natural disaster operations.

(4) Priority 4: Systems use very useful in meeting national emergency, mobilization, or natural disaster operations.

(5) Priority 5: Systems use not essential to support national emergency, mobilization, or natural disaster operations but essential to satisfy other mission/installation support requirements.

(6) Priority 6: Systems use not essential and which could be discontinued or eliminated during the stressed situation.

b. Prioritization schemes are developed as a coordinated effort with users and installation contingency/mobilization planners. Completed prioritization schemes are approved by the installation commander.

c. Denial of services and/or restoration of communications circuits and associated terminal equipment that are assigned NCS restoration priorities is made under policies and procedures established by NCS.

Appendix A
References

Section I
Required Publications

AR 25–1
Army Knowledge Management and Information Technology. (Cited in paras 1–1, 6–5*a*.)

AR 25–2
Information Assurance. (Cited in para 1–1.)

AR 25–10
Reduction and Control of Information Transfer in An Emergency. (Cited in para 7–1*b*.)

AR 70–1
Army Acquisition Policy. (Cited in para 2–3*b*.)

AR 70–75
Survivability of Army Personnel and Materiel. (Cited in para 2–3*b*.)

AR 500–3
U.S. Army Continuity of Operations (COOP) Program Policy and Planning. (Cited in paras 1–1, 1–4.)

Section II
Related Publications
A related publication is a source of additional information. The user does not have to read a related publication to understand this publication. DOD publications are available at www.dtic.mil/whs/directives. U.S. Code is available at www.gpoaccess.gov/uscode.

AR 380–5
Department of the Army Information Security Program

DOD Directive 3020.26
Defense Continuity Programs (DCP)

DOD Directive 8500.1
Information Assurance (IA)

DOD Instruction 3020.42
Defense Continuity Plan Development

DOD Instruction 8500.2
Information Assurance (IA) Implementation

Federal Preparedness Circular 65
Federal Executive Branch Continuity of Operations. (Available at www.gsa.gov.)

NIST Special Publication 800–34
Contingency Planning Guide for Information Technology Systems. (Available at http://csrc.nist.gov/publications/nistpubs.)

OMB Circular A–130
Management of Federal Information Resources. (Available at www.whitehouse.gov/omb.)

10 USC 2224
Defense Information Assurance Program

40 USC 1401
The Clinger-Cohen Act: Definitions

44 USC 3601
Management and Promotion of Electronic Government Service: Definitions

Section III
Prescribed Forms
This section contains no entries

Section IV
Referenced Forms
The following forms are available the APD Web site (www.apd.army.mil) unless otherwise stated.

DA Form 2028
Recommended Changes to Publications and Blank Forms

DA Form 3938
Local Service Request

Appendix B
IT Contingency Plan Template

B–1. General guide
a. This template is for use as a general guide to developing an IT contingency plan.
b. The following elements should be included in the format:
(1) Organization name.
(2) System name.
(3) Date.
(4) Version.
c. Table B–1 demonstrates the format for a document change history.

Table B–1
Document change history

Version #	Change #	Date	Description
Draft	N/A	16 January 2003	Initial draft submission
1	1	5 May 2004	Final version prepared for May 10, 2005 Re-accreditation submission
2	1	13 June 2005	New cover page, incorporated comments identified through the risk assessment report, and added preparation checklist to the applicable appendices

d. For the table of contents, insert the appropriate page and paragraph numbers for the sections developed. The following is a general guide:
(1) Executive summary.
(2) Introduction.
(a) (Insert system name) mission.
(b) Assumption.
(c) Unit responsibility.
(d) Types of emergencies requiring IT contingency plan activation.
(e) System priorities.
1. Overall system priorities.
2. Unit system priorities.
(3) Protection of records and documentation.
(a) List of (insert system name)-specific records and documentation.
(b) Procedures for safeguarding essential materials.

(4) Emergency response.
(a) Telecommunications network.
(b) Service desk.
(c) Hardware failure.
(d) WAN failure.
(e) LAN failure.
(5) Backup operations.
(a) Designation of IT contingency plan site.
(b) Facilities, security, supplies, and information transfer.
1. Facilities
2. Security measure required at the IT contingency plan site.
(c) Personnel requirements.
(d) Planning coordination.
(e) Emergency movement procedures.
(f) Evaluation criteria for IT contingency plan and test methods.
(6) Recovery.
(a) Overview.
(b) Emergency action plans.
(7) Contingency preparations at the host site.
(a) Planning coordination.
(b) Facilities, security, supplies, information transfer, and transportation.
(c) Personnel requirements.
(d) Billeting and messing requirements.
(e) Minimize processing plan.
(f) Evaluation criteria for IT contingency plan and test methods.

B–2. Contingency plan introduction

This document provides contingency guidelines for onsite (INSERT NAME OF SYSTEM) operations. This appendix serves as a guideline for developing contingency planning for each (INSERT NAME OF SYSTEM) operation.

B–3. Mission of (insert name of system)

The (INSERT NAME OF SYSTEM) is a suite of developed, commercial-off-the-shelf and Government-off-the-shelf software applications designed specifically to assist (INSERT NAME OF ORGANIZATION) ommanders and their staffs to (INSERT NAME OF PROCESS) more efficiently. The applications operate in a (INSERT OPERATION SYSTEM) environment on hardware and networks owned, operated, and maintained by the (INSERT NAME OF OPERATION ORGANIZATION). The suite of software automates the (INSERT NAME OF PROCESS). By using these applications, both Joint Forces Headquarters and Regional Readiness Commands improved their preparation for processing at mobilization stations by greatly reducing the time spent on Soldier Readiness Processing for a unit. The Reserve Component Automation System (RCAS) software product is managed by the Project Management Office in Arlington, VA.

B–4. Assumptions

Each organization, under the DODD 3020.26 and AR 500–3, will have a contingency plan for (INSERT NAME OF SYSTEM). The contingency plan will have provisions for the use of alternate sites should a disaster strike. For the purpose of this document, 100 percent implementation of the contingency plan within 12 hours following emergency notification means recovery of those resources that the Unit Commander has deemed to be critical to support essential functions and personnel, as defined by DODD 3020.26 and this pamphlet.

B–5. Unit responsibility

As stated in this pam, the basic responsibility for the contingency plan rests with the unit commander. Within this context, the commander must determine the degree to which the (INSERT NAME OF SYSTEM) is integral to essential operations. (INSERT NAME OF SYSTEM) contingency procedures will be formally documented in a separate plan or may be integrated into an existing unit COOP. For additional information on development of a contingency plan, see DODD 3020.26 and this pamphlet. At a minimum, the (INSERT NAME OF SYSTEM) contingency plan will address the following:

a. Priorities, which establish the order in which (INSERT NAME OF SYSTEM) services will be restored following system outage: The contingency plan will consider priorities for the restoration of services during partial system failure (for example, the loss of one processor at a multiprocessor site), as well as provisions for a total system failure.

b. Procedures for implementing daily backups of modified files and for weekly backups of the entire file system:

Provisions will also be made for the backup of critical system information that is stored on paper (for example, duplicate copies of critical computer or vendor manuals will be maintained).

c. Provisions for offsite storage of backup materials: This requirement reduces the risk of a single event destroying both the primary and backup copies of critical (INSERT NAME OF SYSTEM) electronic data or paper documents. Appropriate security measures will be taken to safeguard backup materials at the offsite storage location. When practical, backup materials should be stored at the alternate processing location.

d. Arrangements made through the chain-of-command to establish alternate processing locations for each (INSERT NAME OF SYSTEM) site: A formal letter or memorandum of agreement to provide support will be developed to establish the conditions and restrictions that govern this arrangement. The roles and responsibilities of the supporting unit and the unit to be supported will be clearly delineated.

e. Additional or special security requirements are necessary at the alternate processing location: Provisions will be made to incorporate these requirements in the unit security standard operating procedures, when required.

f. Identification of personnel who have critical roles in the operation of the (INSERT NAME OF SYSTEM) or in the implementation of contingency plan procedures: Alternate or backup personnel will also be identified for each critical role.

g. Emergency plans or procedures for the protection of the (INSERT NAME OF SYSTEM), sensitive materials, and personnel in the event of fire or natural disaster.

h. Procedures for emergency relocation of RCAS equipment to prevent damage, theft, or compromise.

i. Destruction contingencies for hard drives, floppy diskettes, compact disk read-only memory, tapes and other material, including priorities, procedures, and specific authorities to execute them

j. Provisions for periodic review and revision of the contingency plan by command and managerial personnel to ensure that it is kept up to date.

k. Identification of specific training and testing requirements for all aspects of the contingency plan to ensure its effectiveness when implemented

l. Capability to perform system restores: INSERT THE ABILITY OF THE OPERATING SYSTEM TO PERFORM SYSTEM RESTORES OR UNIQUE FEATURES THAT WOULD FACILITATE RESTORATION WHILE IMPLEMENTING THE CONTINGENCY PLAN

B–6. Types of emergencies requiring contingency plan activation

The following describes types of emergencies that require contingency plan activation:

a. Damage to hardware or communications systems that cause (INSERT NAME OF SYSTEM) to be partially or entirely inoperable during extended periods of time

b. Damage of files that prevent operations

c. Situations that prevent access

d. Conditions that require unit activation and deployment due to a national or state emergency

e. Conditions that destroy a (INSERT NAME OF SYSTEM) facility

B–7. System priorities

a. Overall (INSERT NAME OF SYSTEM) priorities. In systematically prioritizing the restoration of the (INSERT NAME OF SYSTEM) functionality the author must keep in mind that (INSERT NAME OF SYSTEM), as a system, falls into priority Levels 3 or 4 in the organizational priority schema. Priority Levels 3 or 4 allow, at a minimum, 14 days for the restoration of functionality.

(1) *Priority 1: Telecommunications Operations.* The most critical element for (INSERT NAME OF SYSTEM) is the telecommunications system (along with the appropriate Communications Security (COMSEC) procedures and equipment).

(2) *Priority 2: Service Desk.* Assistance is available to help the site bring (INSERT NAME OF SYSTEM) back online.

b. Unit (INSERT NAME OF SYSTEM) priorities. Commanders must identify and document in action plans, those (INSERT NAME OF SYSTEM) functions they believe are critical. The following are suggested priorities:

(1) *Priority 1.* Jobs essential to command functions that are processed interactively or must be processed daily

(2) *Priority 2.* Mission-essential jobs that can be delayed up to two days

(3) *Priority 3.* Jobs that may be delayed up to 14 days

(4) *Priority 4.* Jobs that may be delayed indefinitely or for which a manual backup or alternate-processing procedure exists. The assumption is, if an emergency that has placed the organization in a contingency plan situation is projected to last longer than 14 days, Priority 3 jobs will be deployed to the contingency plan site of operations. The priorities are defined under local requirements and may be expressed in hours rather than days or may require several additional levels of definition.

B–8. Protection of records and documentation

a. List of (INSERT NAME OF SYSTEM)—Specific Records and Documentation. All documents and software required by the (INSERT NAME OF SYSTEM) user to carry out essential functions must be maintained in emergency files, available to alternate headquarters/sites.

b. Procedures for safeguarding essential materials. These include procedures and written instructions, guidelines, and recommendations for performing backup and recovery, which are available through (INSERT NAME OF SYSTEM) site technical guides, contingency plans, and SOP.

B–9. Emergency response

Emergency responses will be defined and documented in each unit's emergency action package.

a. Telecommunications network. Because of the architecture of the (INSERT NAME OF SYSTEM), a disaster experienced by any one unit (or even more than one unit) may not seriously disrupt the continuity of operations of other units. (INSERT NAME OF SYSTEM) functionality that requires communications with other echelons is dependent on the availability of the WAN. The loss of a communications link will be detected by the service desk.

b. Service desk. The service desk has been established in (INSERT NAME AND LOCATION OF FACILITY) to ensure continuity of operations for the (INSERT NAME OF SYSTEM) support.

c. Hardware failure. In the event of hardware or component failure hosting the (INSERT NAME OF SYSTEM) software applications, notify the higher headquarters or the supporting system administrator or director of information management representative.

d. WAN failure. Each domain is independent from other domains and does not depend on the WAN for most operations. Operations may continue within a domain even if the WAN experiences an outage. However, outages at Joint Forces Headquarters/Regional Readiness Command sites can impact subordinate elements. In the event of a WAN outage, each site should open a trouble to the appropriate help desks.

e. LAN failure. In the event that a LAN outage occurs, notify the next higher headquarters information assurance program manager, system administrator, director of information management representative, or service desk. The appropriate command level will conduct investigation and repair.

B–10. Backup operations

a. Designation of contingency plan site. The unit will determine alternate headquarters/sites for (INSERT NAME OF SYSTEM) units. Because of the various (INSERT NAME OF SYSTEM) configurations, it is essential that technically compatible sites be chosen. The target recovery site computing capabilities must, at a minimum, be equivalent to those of the original (INSERT NAME OF SYSTEM) unit.

b. Facilities, security, supplies, and information transfer.

(1) *Facilities.* Define and document office space and equipment needed for supporting the additional (INSERT NAME OF SYSTEM) personnel from the affected site.

(2) *Security measures required at the contingency plan site.* Unclassified SENSITIVE (INSERT NAME OF SYSTEM) processing will occur where current operational area and mobilization activities occurs using existing safeguards, which are in compliance with AR 380–5, AR 25–2, and the accreditation document.

(a) Hardware. Security containers should be available for sites with classified removable hard drives. Removable hard drives and encryption keys will be safeguarded in accordance with current guidelines, AR 380–5, chapter 5.

(b) Software. The operating system allows processing up to sensitive information.

(c) Data. Unclassified processing will occur on a compatible (INSERT NAME OF SYSTEM) configuration where current unclassified operational area and mobilization activities occur. The (INSERT NAME OF SYSTEM) database configuration will assure that data from the affected site is not intermixed with those of the contingency plan site.

(d) Technical considerations. Once the alternate operating site has been selected, check with that site's information assurance security officer to identify any additional measures that you must take (for example, setting up user names in advance) to make sure that the stricken site can access its data on the contingency plan site's Reserve Component automation system in the event of an emergency.

c. Personnel requirements. List by functional position those personnel to support each contingency affecting the Reserve Component automation system. Annex D of the unit's (INSERT NAME OF SYSTEM) contingency plan provides the contact information.

d. Planning coordination. The unit commander and information assurance security officer have responsibilities regarding planning coordination.

e. Emergency movement procedures. The unit is responsible for including (INSERT NAME OF SYSTEM) requirements into its existing movement procedures. This includes retrieval of backup files and databases and their transportation to the contingency plan site.

f. Evaluation criteria for contingency plan and test methods. The following describes the evaluation criteria for the contingency plan and test methods:

(1) Review plans and procedures for the periodic test of the contingency plan.

(2) Review documentation detailing when and how the contingency plan has been executed.

(3) Review emergency response procedures.

(4) Verify emergency workload priorities. A list of priority work should be established so that important work continues to be done, if possible.

(5) Review alternate procedures for processing priority work.

(6) Use alternate procedures to ensure that priority workloads could be satisfied.

(7) Conduct an emergency response drill.

(8) Ensure that the contingency plan contains a valid and current (within 12 months) MOA with a contingency plan site.

(9) Verify contingency plan site hardware/software compatibility.

(10) Verify list of required personnel for deployment to the alternate site.

(11) Ensure adequate facilities and services are available for your personnel while operating at the contingency plan site.

(12) Ensure adequate vehicles have been identified and are operational, should the need for deployment arise.

(13) Verify communications arrangements for deployment to the contingency plan site.

(14) Maintain inventory supplies.

(15) Ensure the contingency plan describes policies and procedures to maintain supplies at the alternate site of operations.

(16) Review procedures for maintenance of backup materials.

(17) Maintain inventory backup materials.

(18) Execute the contingency plan.

(19) Review recovery plans.

B–11. Recovery

a. Overview. Continual assessment of the operational and functional status of the (INSERT NAME OF SYSTEM) software applications will be made during the disaster recovery process, and this assessment will be compared to the predisaster operating capability. When, in the opinion of the unit commander, an acceptable level of service has been obtained, the disaster recovery process will be terminated. Once the disaster status has been terminated and operations have been restored, the disaster will be analyzed and documented. This record will contain those actions taken while restoring the affected RCAS capability, as well as providing recommendations for improving future disaster operation recovery planning.

b. Emergency action plans. An emergency action plan will be developed and maintained by the unit for use by emergency staff personnel. This plan will detail the responsibilities of recovery participants, provide current team contact lists, and contact lists of other key organization managers and entities that might be required. This plan will also contain emergency action checklists that define the required actions; a roster of essential personnel (and alternates), including their emergency function assignments and locations; a listing of documents and records required to be readily available at the emergency sites; and other data required in an emergency. Units will document reviews, tests, and drills of their plan annually.

B–12. Contingency operations at the host site

a. Planning coordination. The unit commander and IASO have responsibilities regarding planning coordination. The unit commander must ensure that the necessary agreements have been made and the IASO must coordinate the (INSERT NAME OF SYSTEM) specific technical requirements.

b. Facilities, security, supplies, information transfer, and transportation. Office space and equipment at the contingency plan site must support the additional personnel who will be using the (INSERT NAME OF SYSTEM). Comparable safeguards for the storage and processing of classified and unclassified sensitive information and material, including Security Command material, must be in place. Administrators and information assurance personnel must plan methods to ensure that data from the affected site is not intermixed with that of the contingency plan site. Coordination will include identifying any additional measures required to make sure personnel from the stricken site can access their data at the contingency plan site. As per the processing priorities under contingency plan conditions, the contingency plan site will adjust its workload to ensure that critical and essential data from both the affected site and the contingency plan site can be processed.

c. Personnel requirements. If the host at the contingency plan site has agreed to provide personnel support, a list by title, grade, and number of the contact information should be obtained of those personnel available to support the affected unit. Include other special requirements, if needed.

d. Billeting and messing requirements. It should be ensured that billeting and messing requirements are augmented to provide for the additional personnel using the (INSERT NAME OF SYSTEM), if needed.

e. Minimize processing plan. As per the processing priorities under contingency plan conditions, the host workload should be adjusted to ensure that critical and essential data from both the affected site and the host site can be processed.

f. Evaluation criteria for contingency plan and test methods. The host site will review plans and procedures for the periodic testing of the contingency plan and will execute those plans to ensure all requirements can be met. The criteria for evaluating the contingency plan at the host site will parallel the evaluation criteria used by the affected site.

Glossary

Section I
Abbreviations

AKO
Army Knowledge Online

AR
Army regulation

ATM
asynchronous transfer mode

BCP
business continuity plan

BIA
business impact analysis

BRP
business recovery plan

CAC
common access card

CD
compact disc

CD–ROM
compact disc-read only memory

C4
command, control, communications, and computers

CIO/G–6
Chief Information Officer/G–6

CONOPS
concept of operations

COOP
continuity of operations

COTS
commercial-off-the-shelf

DA
Department of the Army

DASD
direct access storage device

DNS
domain name server

DOD
Department of Defense

DODD
Department of Defense Directive

DOIM
director of information management

DRP
disaster recovery plan

DVD
digital video disc

EAC
emergency action console

GETS
Government Emergency Telephone Service

IA
information assurance

IP
Internet Protocol

iSCSI
internet small computer system interface

ISDN
integrated services digital network

IT
information technology

LAN
local area network

Mbps
Megabits per second

MC/ME
mission critical/mission essential

MEF
mission essential function

MOA
memorandum of agreement

MOU
memorandum of understanding

MS
mobilization station

MWR
morale, welfare, and recreation

NAS
network attached storage

NCS
National Communications System

NIPRNet
Unclassified but Sensitive Internet Protocol Router Network

NSP
network service provider

OEP
occupant emergency plan

OMB
Office of Management and Budget

Pam
pamphlet

PC
personal computer

PDD
Presidential Decision Directive

P.L.
Public Law

POC
point of contact

RAID
redundant arrays of independent disks

RCAS
Reserve Component Automation System

RMT
risk management team

RPO
recovery point objectives

RTO
recovery time objectives

SAN
storage area network

SIPRNet
Secret Internet Protocol Router Network

SLA
service level agreement

SONET
synchronous optical network

UPS
uninterrupted power supply

URL
uniform resource locator

USC
United States Code

VPN
virtual private network

WAN
wide-area network

WPS
wireless priority service

Section II
Terms

IT contingency statement
A formal organization policy that provides the authority and guidance necessary to develop an effective contingency plan.

Alternate site
A location to recover and perform system operations for an extended period in the event of IT Contingency Plan implementation. In general, three types of alternate sites are available: (1) A dedicated site owned or operated by the organization; (2) A site reserved via reciprocal agreement or memorandum of agreement with an internal or external entity; (3) A commercially leased facility.

Business continuity plan (BCP)
A plan to sustain an organization's business functions during and after a disruption. IT systems are considered in the BCP in terms of their support to the business processes.

Business impact analysis (BIA)
A plan that assists contingency team members identify and prioritize critical IT systems and components.

Business recovery plan (BRP)
Addresses the restoration of business processes after an emergency but, unlike the BCP, does not include procedures to ensure the continuity of critical processes throughout the emergency or disruption. Also known as the Business Resumption Plan.

Cold site
A facility with adequate space and infrastructure (electric power, telecommunications connections, and environmental controls) to support the IT system. The space may have raised floors and other attributes suited for IT operations. The site does not contain IT equipment and usually does not contain office automation equipment, such as telephones, facsimile machines, or copiers. The organization using the cold site is responsible for providing and installing necessary equipment and telecommunications capabilities.

Command and control
Exercise of authority and direction by a properly designated commander over assigned forces in the accomplishment of the mission. These functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures that are employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission.

Contingency planning coordinator
The person with the responsibility for the overall contingency planning process and is typically a functional or resource manager within the agency.

Continuity of operation (COOP) plan
Provide procedures and capabilities to sustain an organization's essential, strategic functions for up to 30 days

Continuity of support/IT contingency plan
Plans for general support systems and contingency plans for major applications. Because an IT contingency plan should

be developed for each major application and general support system, multiple contingency plans may be maintained within the organization's BCP.

Cyber incident response plan
Provides strategies to detect, respond to, and limit consequences of malicious cyber incident.

Differential backup
A backup that stores files created or modified since the last full backup.

Disaster recovery plan (DRP)
Applies to major, usually catastrophic, events that deny access to the normal facility for an extended period. Frequently, DRP refers to an IT-focused plan designed to restore operability of the target systems, applications, and an IT contingency plan; however, the DRP is narrower in scope and does not address minor disruptions that do not require relocation.

Electronic vaulting
Provides additional data backup capabilities, with backups made to remote tape drives over communication links. Electronic vaulting enables shorter recovery times and reduced data loss should the server be damaged between backups. The system is connected to an electronic vaulting provider to allow backups to be created offsite automatically. With this technology, data is transmitted to the electronic vault as changes occur on the servers between regular backups. These transmissions between backups are sometimes referred to as electronic journaling. (See also remote journaling)

Full backup
A backup that captures all files on the disk or within the folder selected for backup. Because all backed-up files were recorded to a single media or media set, locating a particular file or group of files is simple. However, the time required to perform a full backup can be lengthy. In addition, full backups of files that do not change frequently (such as system files) could lead to excessive, unnecessary media storage requirements.

Hot site
Office spaces appropriately sized to support system requirements and configured with the necessary system hardware, supporting infrastructure, and support personnel. Hot sites are typically staffed 24 hours a day, 7 days a week. Hot site personnel begin to prepare for the system arrival as soon as they are notified that the contingency plan has been activated.

Incremental backup
Captures files that were created or changed since the last backup, regardless of backup type. Incremental backups afford more efficient use of storage media, and backup times are reduced. However, to recover a system from an incremental backup, media from different backup operations may be required. For example, consider a case in which a directory needed to be recovered. If the last full backup was performed three days prior and one file had changed each day, then the media for the full backup and for each day's incremental backups would be needed to restore the entire directory.

Internet backup/online backup
A strategy that allows PC users to back up data to a remote location over the Internet. A utility is installed onto the PC that allows the user to schedule backups, select files and folders to be backed up, and establish an "archiving" scheme to prevent files from being overwritten. Data can be encrypted for transmission; however, this will impede the data transfer speed over a modem connection. The advantage of Internet Backup is that the user is not required to purchase data backup hardware or media.

Mirrored site
Fully redundant facilities with full, real-time information mirroring. Mirrored sites are identical to the primary site in all technical respects. These sites provide the highest degree of availability because the data is processed and stored at the primary and alternate site simultaneously. These sites typically are designed, built, operated, and maintained by the organization.

Mission essential functions (MEFs)
Functions that enable the installation DOIM to provide vital services and sustain the post's IT infrastructure in an emergency.

Mobile site
Self-contained, transportable shells custom-fitted with specific telecommunications and IT equipment necessary to meet system requirements. These are available for lease through commercial vendors. The facility often is contained in a tractor-trailer and may be driven to and set up at the desired alternate location. In most cases, to be a viable recovery solution, mobile sites should be designed in advance with the vendor, and an SLA should be signed between the two parties. This is necessary because the time required to configure the mobile site can be extensive, and without prior coordination, the time to deliver the mobile site may exceed the system's allowable outage time.

Notification/activation phase
Defines the initial actions taken once a system disruption or emergency has been detected or appears to be imminent. This phase includes activities to notify recovery personnel, assess system damage, and implement the plan.

Occupant emergency plan (OEP)
Provides the response procedures for occupants of a facility in the event of a situation posing a potential threat to the health and safety of personnel, the environment, or property.

Parity
A technique of determining whether data has been lost or overwritten. Parity has a lower fault tolerance than mirroring. The advantage of parity is that data can be protected without having to store a copy of the data, as is required with mirroring.

Recovery phase
Segment of the IT contingency plan in which activities focus on contingency measures to execute temporary IT processing capabilities, repair damage to the original system, and restore operational capabilities at the original or new facility.

Recovery point objective (RPO)
The RPO is the point in time in which data must be restored in order to resume processing.

Recovery time objective (RTO)
Maximum acceptable length of time that elapses before the unavailability of the system severely affects the organization.

Redundant arrays of independent disks (RAID)
Provides disk redundancy and fault tolerance for data storage and decreases mean time between failures. RAID is used to mask disk drive and disk controller failures. In addition, RAID increases performance and reliability by spreading data storage across multiple disk drives, rather than a single disk. RAID can be implemented through hardware or software; in either case, the solution appears to the operating system as a single logical hard drive. With a RAID system, hot swappable drives can be used-that is, disk drives can be swapped without shutting down the system when a disk drive fails.

Remote journaling
Provides additional data backup capabilities, with backups made to remote tape drives over communication links. With remote journaling, transaction logs or journals are transmitted to a remote location. If the server needed to be recovered, the logs or journals could be used to recover transactions, applications, or database changes that occurred after the last server backup. Remote journaling can either be conducted through batches or be communicated continuously using buffering software. Remote journaling and electronic vaulting require a dedicated off-site location to receive the transmissions. The site can be the system's hot site, off-site storage site, or another suitable location. (See also electronic vaulting)

Risk assessment
Identifies an organization's information assets and the threats to each asset.

Risk management
An ongoing commitment essential to effective risk management. Risk management includes an array of activities used to identify, control, and mitigate risks to IT systems and the ability to provide IT services.

Server load balancing
Means to increases server and application availability. Through load balancing, traffic can be distributed dynamically across groups of servers running a common application so that no one server is overwhelmed. With this technique, a group of servers appears as a single server to the network. Load balancing systems monitor each server to determine

the best path to route traffic to increase performance and availability so that one server is not overwhelmed with traffic. Load balancing can be implemented among servers within a site or among servers in different sites. Using load balancing among different sites can enable the application to continue to operate as long as one or more sites remain operational. Thus, load balancing could be a viable contingency measure depending on system availability requirements.

Service level agreement (SLA)
A formal agreement between the customer(s) and the service provider specifying service levels and the terms under which a service or a package of services is provided to the customer.

Striping
A method of improving the performance of the hardware array controller by distributing data across all the drives. In striping, a data element is broken into multiple pieces, and a piece is distributed to each hard drive. Data transfer performance is increased using striping because the drives may access each data piece simultaneously. Striping can be implemented in bytes or blocks. Byte-level striping breaks the data into bytes and stores the bytes sequentially across the hard drives. Block-level striping breaks the data into a given-size block, and each block is distributed to a disk.

Vital records
Records required for the Army to conduct its business under other than standard operating conditions, to resume normal business afterward, and to identify and protect important records dealing with the legal and financial rights of the Army and persons directly affected by actions of the Army.

Warm site
Partially equipped office spaces that contain some or all of the system hardware, software, telecommunications, and power sources. The warm site is maintained in an operational status ready to receive the relocated system. The site may need to be prepared before receiving the system and recovery personnel. In many cases, a warm site may serve as an operational facility for another system or function, and in the event of contingency plan activation, the standard activities are displaced temporarily to accommodate the disrupted system.

Section III
Special Abbreviations and Terms
This section contains no entries.

USAPD

ELECTRONIC PUBLISHING SYSTEM
OneCol FORMATTER WIN32 Version 235

PIN:	083586–000
DATE:	11-16-06
TIME:	10:09:33
PAGES SET:	67
DATA FILE:	C:\wincomp\p25-1-2.fil
DOCUMENT:	DA PAM 25–1–2
SECURITY:	UNCLASSIFIED
DOC STATUS:	NEW PUBLICATION